

# 2  
500.40368X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : HONJO, et al

Serial No.: Not assigned

Filed: July 20, 2001

Title: ACCESS CONTROL METHOD

Group: Not assigned

JG978 U.S. PRO  
09/909006  
07/20/01

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

July 20, 2001

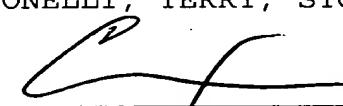
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2000-320645 filed October 20, 2000.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
Carl I. Brundidge  
Registration No. 29,621

CIB/amr  
Attachment  
(703) 312-6600

日本国特許庁  
JAPAN PATENT OFFICE

JC97® U.S. PRO  
09/909006  


別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日  
Date of Application: 2000年10月20日

出願番号  
Application Number: 特願2000-320645

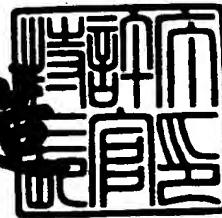
出願人  
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 6月 6日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕三



【書類名】 特許願  
【整理番号】 K00018781  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 9/00  
【発明者】  
【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内  
【氏名】 本城 信輔  
【発明者】  
【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内  
【氏名】 洲崎 誠一  
【特許出願人】  
【識別番号】 000005108  
【氏名又は名称】 株式会社日立製作所  
【代理人】  
【識別番号】 100077274  
【弁理士】  
【氏名又は名称】 磯村 雅俊  
【電話番号】 03-3348-5035  
【復代理人】  
【識別番号】 100102587  
【弁理士】  
【氏名又は名称】 渡邊 昌幸  
【電話番号】 03-3348-5035  
【手数料の表示】  
【予納台帳番号】 068262  
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003100

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人情報の信頼度および開示度による認証またはアクセス管理システム、および管理方法

【特許請求の範囲】

【請求項1】 ネットワークに接続されたユーザ端末と、

該ユーザ端末からのチケット発行要求に応じて、個人情報データベースに登録された当該ユーザの個人情報を取出し、チケットを作成して該ユーザ端末に返送するチケット発行サーバと、

必要な情報、該情報の開示レベルおよび該情報の承認の要不要を内容とするサーバ・ポリシを設定し、アクセス条件が要チケットの場合には、各ユーザ端末に該サーバ・ポリシと要チケットを通知して、アクセス要求を受信した場合には、添付されたチケットの内容と該サーバ・ポリシを照合してアクセス可能か否かを判別するアクセス制御サーバと

を有することを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理システム。

【請求項2】 請求項1に記載の個人情報の信頼度および開示度による認証またはアクセス管理システムにおいて、

前記チケットは、一つ以上の個人情報および該個人情報に関する属性情報を記載したデータと、該チケットの発行元の第三者機関によって該データに施されたデジタル署名とを内容とし、

アクセス制御サーバが示すポリシに従って開示情報を制御する証明書であり、該アクセス制御サーバにより検証されることを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理システム。

【請求項3】 クライアントからのアクセス要求を受信すると、アクセス制御に要チケットか否か、該アクセス要求にチケットが添付してあるか否か、該チケットが正当なものであるか否か、当初設定したサーバ・ポリシと照合して一致するか否か、をそれぞれ判別することにより、アクセス制御を行うことを特徴とするアクセス制御サーバ装置。

【請求項4】 クライアントからのチケット要求を受信すると、該チケット要求に添付されたサーバ・ポリシおよびアクセス希望ディレクトリを解析し、希望ディレクトリにアクセスするために必要な個人情報、承認の必要性、および開示の必要性を調べ、データベースから必要な情報を取得してチケットを作成し、作成したチケットを上記クライアントに送信することを特徴とするチケット発行サーバ装置。

【請求項5】 アクセス制御サーバはサーバ・ポリシを設定し、クライアントからのアクセス要求を受けると、アクセスに要チケットか否かを確認して、要チケットの場合にはチケット要求と上記サーバ・ポリシを該クライアントに通知し、

該クライアントはチケット発行サーバに上記サーバ・ポリシを添付してチケット要求を送信し、

該チケット発行サーバは、該サーバ・ポリシを解析して必要な情報を用いてチケットを生成し、該クライアントに生成したチケットを送信し、

該クライアントは受信したチケットを保存するとともに、該チケットを添付してアクセス制御サーバにアクセス要求を送信し、

該アクセス制御サーバは、添付されたチケットを検証するとともに、該サーバ・ポリシと照合して検証することにより、アクセスを許可または不許可とすることを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理方法。

【請求項6】 チケット発行サーバは、クライアントからのチケット要求を受信すると、セッション鍵を生成し、必要な情報および該セッション鍵を記載したチケットを発行し、該チケットをアクセス制御サーバの公開鍵で暗号化し、暗号化したチケットとセッション鍵を上記クライアントに送信し、

該クライアントは、受信したチケットとセッション鍵を保存するとともに、該セッション鍵でアクセス要求時刻を暗号化して認証子を作成し、アクセス制御サーバに対して該認証子と暗号化されたチケットとを添付してアクセス要求を送信し、

該アクセス制御サーバは、上記暗号化されたチケットを復号化して、該チケッ

トからセッション鍵を取り出し、該セッション鍵で該認証子を復号化し、得られた時刻を検証するとともに、該チケットおよびサーバ・ポリシを検証して、アクセスを許可するか否かを決定することを特徴とする個人情報の信頼度および開示度による認証またはアクセス管理方法。

【請求項7】 請求項5または6に記載の個人情報の信頼度および開示度による認証・アクセス管理方法の各処理ステップをプログラムに変換し、該プログラムを記録媒体に格納したことを特徴とするコンピュータにより読み出し可能なプログラム記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、信頼のある個人情報をもとに個人情報を秘匿してアクセス管理を行うことを可能にした個人情報の信頼度および開示度による認証またはアクセス管理システムおよび管理方法に関する。

##### 【0002】

##### 【従来の技術】

従来、認証方法としてはユーザIDやパスワードを使用した認証方法、または公開鍵暗号系を使用する方法（例えば、SSL（Secure Socket Layer）が用いられてきた。

ユーザIDやパスワードによる認証方法は、あらかじめ登録されたユーザIDやパスワードに合致することを検証する方法と、ユーザIDとパスワードから秘密鍵を生成して、これを保持していることを証明することによって検証する方法がある。

公開鍵暗号系では、暗号系と復号化に異なった鍵を用い、復号鍵を秘匿しており、暗号鍵を公開する。

公開鍵暗号系における認証は、この暗号鍵を保持していることを何らかの形で証明することで行われる。

この公開された暗号鍵は、名前、組織名、有効期限などの情報とともに、公開鍵証明書に格納され、この公開鍵証明書を参照することにより認証する相手の身

元の情報を得ることができる。

#### 【0003】

##### 【発明が解決しようとする課題】

しかしながら、従来の認証・アクセス方法では、下記のような問題点があった。  
1) ユーザの身元がわかつてしまうこと、すなわち、認証技術であるから当然のことであるが、身元を明かして認証をもらう必要がある。しかし、匿名で投稿をしたいときや、身元を隠して掲示板に書き込みたいときなど、身元を隠してアクセスしたい場合があるが、従来の方法では認証が受けられないという問題があった。

2) ユーザ登録が必要であること、すなわち、予めアクセスを許可するユーザを決めておく必要がある。しかし、身元を確実にすることは必要であるが、アクセスする際だけは身元を隠しておきたい場合があるという問題がある。

3) ユーザのアクセス許可の設定が一元的であること、すなわち、認証側では、登録されたユーザIDだけを検証して、許可するか否かの判断材料になっていた。しかし、ユーザ側としては、他の情報も判断の材料にしたいという要望がある

#### 【0004】

例えば、女性だけアクセスを許可する掲示板を設置したい場合があるが、このときには性別のみの認証を得ていればよいことになる。また、18才以上の者しか見られない成人向けのサイトを設置する場合には、18才以上という年令のみの認証を得ていればよいことになる。また、匿名の投稿をしたいときには、アクセスされる側としては、誹謗中傷など問題のあった場合に送信者が特定できる必要がある。また、匿名のハンドル名で何回か投稿されたときに、それらが本当に同じ送信者によるものであることを保証する方法があればよい訳である。

しかし、従来の認証技術では、性別のみの認証、年令のみの認証はできなかつた。また、他人によるなりすましが可能になっていた。

#### 【0005】

そこで、本発明の目的は、これら従来の課題を解決し、信頼のある個人情報をもとにアクセス管理を行い、かつ個人情報を秘匿してアクセスが可能な個人情報

の信頼度および開示度による認証またはアクセス管理システム、および管理方法を提供することにある。

#### 【0006】

##### 【課題を解決するための手段】

上記目的を達成するため、本発明の認証またはアクセス管理システムは、ネットワークに接続されたユーザ端末と、該ユーザ端末からのチケット発行要求に応じて、個人情報データベースに登録された当該ユーザの個人情報を取出し、チケットを作成して該ユーザ端末に返送するチケット発行サーバと、必要な情報、該情報の開示レベルおよび該情報の承認の要不要を内容とするサーバ・ポリシを設定し、アクセス条件が要チケットの場合には、各ユーザ端末に該サーバ・ポリシと要チケットを通知して、アクセス要求を受信した場合には、添付されたチケットの内容と該サーバ・ポリシを照合してアクセス可能か否かを判別するアクセス制御サーバとを有することを特徴としている。

上記チケットは、一つ以上の個人情報および該個人情報に関する属性情報を記載したデータと、発行元の第三者機関によって該データに施されたデジタル署名から構成されるもので、ポリシーに従って開示情報を制御した証明書とみなすことができる。

個人情報はサーバ・ポリシに従ってチケットに直接記載するか、または、直接記載しない場合は開示しない旨をチケットに記載する。

また、該個人情報に関する属性情報の例としては、個人情報の信頼度、すなわち該個人情報が第三者機関によって承認された情報であるか否かを示す情報が挙げられる。

個人情報の信頼度の設定の方法は、例えば、生年月日を登録時に確認する第三者機関は、生年月日を承認された情報としてチケットに設定できるが、登録時に生年月日の確認を行わない第三者機関は、生年月日を未承認な情報としてチケットに設定する。

#### 【0007】

##### 【発明の実施の形態】

以下、本発明の原理および実施例を、図面により詳細に説明する。

## (原理)

- 本発明の認証またはアクセス管理方法は、次の手順で行われる。
- 1) 個人情報を第三者機関に登録する。これは、従来の認証技術と同じである。
  - 2) アクセス制御を行うサーバに、その条件を記載したサーバ・ポリシを設定する。サーバ・ポリシの記載内容としては、対象ディレクトリ、必要な情報（例えば、名前や生年月日）、情報の開示レベル（名前を記載する必要があるか？）、情報の承認が必要か否か？例えば、`http://www.abc.com/cgi-bin/abc`（名前、開示不要、要承認）、（生年月日、要開示、要承認）
  - 3) 利用者は、第三者機関に必要な情報を承認してもらうために、チケットを発行してもらう。チケットの内容の例としては

(名前：非開示：承認、

生年月日：1969.9.17:承認

第三者機関：A B C)

- 4) 利用者は、チケットをサーバに提示、サーバは、チケットの内容とサーバ・ポリシとを照らし合わせ、アクセス可能か否かを判断する。

上記の例の場合には、第三者機関A B Cによって、名前が承認されており、生年月日が開示され、かつ承認されているので、アクセスを許可する。

- 5) 特に、匿名アクセス許可の後、問題が発生すれば、被害者または裁判所などの調停者はサーバ上の掲示板に、送信者に不適正な書き込みがあることを伝えることにより、サーバはチケット記載の情報を第三者機関に問い合わせ、第三者機関は送信者を特定し、特定した者に警告など所定の対処を施し、調停者などに対所を施したこと伝えるか、あるいは送信者の情報を提供する。

## 【0008】

図1は、本発明の原理（解決手段1）を示す説明図であって、承認されたハンドル名によるアクセス制御の場合を示す。

図1において、10は信頼できる第三者機関A B Cであって、個人情報データベース11を備えている。11Aは、個人情報データベースに登録された内容である。20はユーザ（ここでは`honjo`）、12は第三者機関A B C 10によ

り発行されたチケット内容、30はアクセスを制御するサーバであって、31はサーバ・ポリシの内容、31Aはサーバ・ポリシの送信内容である。

以下、①～⑦の手続きの番号に従って処理手順を説明する。先ず、①ユーザ20は、第3者機関ABC12に対して個人情報の登録を行う。ここには、例えば、ユーザID、氏名、生年月日、住所、性別、ハンドル名が登録されている。次に、②ユーザ20は、サーバ30に対して掲示板Aに書き込み希望を送信する。

アクセス制御サーバ30は、サーバ・ポリシ31として、掲示板A：認証されたハンドル名でアクセスすること、化粧品ページB：アクセスできるのは女性であること、成人向けページC：アクセスできるのは18才以上であること、を持っている。③サーバ30は、ユーザ20からの掲示板Aへの書き込み希望に対して、サーバ・ポリシの内容31Aとチケットが必要である旨を返送する。

④ユーザ20は、第三者機関ABC10に対してチケット発行希望（認証されたハンドル名を記載）する。⑤第3者機関ABC10は、チケット発行希望があると、個人情報データベース11の内容を参照して、チケット12をユーザに送信する。チケット12の内容は、チケットIDと、ハンドル名（J b o y）が第3者機関ABCにより承認されていることを記載して、改ざん防止のためにABCによるデジタル署名を行う。

⑥ユーザは、アクセス制御サーバ30に対して、発行されたチケット12を添付して、掲示板Aへの書き込み希望を送信する。⑦アクセス制御サーバ30は、チケット12を検証し、アクセスの確認を行い、メッセージを返送する。

#### 【0009】

図2は、同じく原理（解決手段1）の承認されたハンドル名によるアクセス制御において、不適正な書き込みをした場合の手続を示す図である。

図1の手続において、ハンドル名J b o yが不適正な書き込み、例えば他人の中傷誹謗を書き込んだ場合、重大な不法行為をする決意を書き込んだ場合には、被害者または裁判所などの調停者70は、①サーバ上の掲示板に、J b o yによる不適正な書き込みがあることをサーバ30に伝える。②アクセス制御サーバ30は、該当する書き込みを特定し、対応するチケットIDを特定する。③サーバ30は、第三者機関ABC10に対して、J b o yが不適正な書き込みをした

ことを伝える。チケットIDを送信する。④第三者機関ABC10は、個人情報データベース11を検索して、Jboyは、ユーザhonioであることが分かる。⑤第三者機関ABC10は、ユーザ20に対して警告を与える。⑥第三者機関10は、送信者を特定した後、被害者または調停者70に対して、送信者にかかるべき対処を施したことなどを伝える。状況によっては、調停者70に送信者の情報を提供することもある。

この結果、インターネットにおいて、個人情報を秘匿しても、本発明では身元保証が可能であるため、無責任な行動や犯罪が少なくなる。

#### 【0010】

図3は、本発明の原理（解決手段2）を示す説明図であって、性別によるアクセス管理を示す。

①ユーザ20は、サーバ30に対して化粧品ページBに書き込み希望を送信する。②サーバ20は、化粧品ページBは女性だけがアクセスできる、というサーバ・ポリシ31があること、要チケットであること、をユーザ20に送信する。③ユーザ20は、第三者機関ABC10に対してチケット発行希望（性別の証明）を送信する。④第三者機関ABC10はチケット発行希望があると、個人情報データベース11の内容を参照して、チケット12を発行し、ユーザ20に送信する。チケット12には、チケットIDと、このユーザは女性であることを記載し、ABCによるデジタル署名を行う。⑤ユーザ20は、サーバ30に対しチケット12を添付して化粧品ページBへの書き込み希望を送信する。⑥サーバ30は、チケットを検証し、女性であるので、このアクセスを許可し、⑦ユーザ20に対して化粧品ページBを送信する。なお、不許可の場合には、化粧品ページBを送信せずに、エラーメッセージを送信する。

#### 【0011】

（実施例1）

（ネットワーク構成）

図4は、本発明の実施例1を示すネットワークの構成図である。

図4において、40は会社や大学等の私有の閉じられたネットワーク（いわゆるインターネット）であり、50はインターネット、30はインターネット50

に接続されたWWWサーバである。10はチケット発行サーバであって、個人情報データベース11を備えている。この場合、個人情報を把握している会社の人事課などがチケット発行サーバ10になれば、都合がよい。20はクライアントであって、WWWブラウザ22に新たにチケット処理プラグインプログラム21が追加されている。WWWサーバ30には、サーバ・ポリシ31が備えられるとともに、新たにチケット認証・アクセス管理部32が設けられる。従来のブラウザ22は、チケットを使えないため、チケットを使えるようにチケット認証・アクセス管理部32を設けるとともに、チケット処理プラグインプログラム21をブラウザ32に付加される。

なお、将来、市町村の役所や個人情報を把握した団体などがチケット発行サーバ10になる場合には、閉じたネットワーク40に設置することなく、インターネット50に直接設置することができる。

### 【0012】

#### (クライアント構成)

図5は、図4におけるクライアントの詳細構成図である。

クライアント（端末）は、通信ケーブルを介してインターネットに接続されており、ネットワークインターフェース28を経由してメインバスに接続される。メインバスには、端末全体を制御するCPU24、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク25、インターネットの各情報などを表示する表示装置26、マウスなどの入力装置27が接続されている。メインメモリには、オペレーティングシステム23、WWWブラウザプログラム22およびチケット処理プラグインプログラム21が格納される。チケット処理プラグインプログラム21を実行することにより、第三者機関10へのチケット発行要求や個人情報の登録などを自動的に行うことができる。

### 【0013】

#### (チケット発行サーバ構成)

図6は、図4におけるチケット発行サーバの詳細構成図である。

チケット発行サーバ10は、通信ケーブルを介してインターネットに接続されており、ネットワークインターフェース17を経由してメインバスに接続される。

メインバスには、サーバ全体を制御するCPU14、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク11、表示装置15、入力装置16が接続されている。メインメモリには、オペレーティングシステム12とチケット発行プログラム13が格納されている。チケット発行プログラム13を実行することにより、通信ケーブルを介してチケット発行要求が送られてきたときには、自動的に一つ以上の押人情報とその個人情報に関する属性情報を記載し、発行元の第三者機関のデジタル署名を記載することができる。

#### 【0014】

(WWWサーバ構成)

図7は、図4におけるWWWサーバの詳細構成図である。

WWWサーバ（アクセス制御サーバ）30は、通信ケーブルを介してインターネットに接続されており、ネットワークインターフェース39を経由してメインバスに接続される。

メインバスには、サーバ全体を制御するCPU35、プログラムなどを格納するメインメモリ、外部メモリであるハードディスク36、表示装置37、入力装置38が接続されている。メインメモリには、オペレーティングシステム34と、WWWサーバプログラム33と、チケット認証・アクセス管理プログラム32とが格納されている。このチケット認証・アクセス管理プログラム32を実行することにより、通信ケーブルを介して掲示板などに書き込みするためのアクセス要求が送られてきたときに、自動的にチケットの認証およびアクセス管理を行うことができる。

#### 【0015】

(個人情報データベース)

図8は、本発明の実施例1を示す個人情報データベースのデータ構成図である。

図8に示すように、個人情報データベースには、ユーザID、氏名、連絡先（住所）、生年月日、性別、ハンドル名、所属、メールアドレス、が記載されている。

#### 【0016】

(サーバ・ポリシ)

図9は、本発明の実施例1を示すサーバ・ポリシの内容例を示す図である。

サーバ：www. a b c. com. のサーバ・ポリシとして、3つの例が記載されている。

1) サービス：掲示板

必要な情報：ハンドル名、要承認、開示

必要な情報：氏名、要承認、非開示

必要な情報：連絡先、要承認、非開示

(この掲示板には、承認が必要であり、かつ開示が必要なハンドル名と、開示する必要はないが、承認が必要な氏名と、開示する必要はないが、承認が必要な連絡先とが必要な情報となっている。)

2) サービス：女性専用ページ

必要な情報：ハンドル名、要承認、開示

必要な情報：性別＝‘女’、要承認、開示

(このページには、承認が必要であり、かつ開示が必要なハンドル名と、承認が必要で、かつ開示も必要な‘女’である性別情報が必要な情報となっている)

3) サービス：映画情報ページ（暴力シーン・性的なシーンあり）

必要な情報：年令 $\geq$ ‘18’、要承認、開示

(このページには、承認が必要であり、かつ開示が必要な‘18才’という年令が必要な情報となっている)

また、サーバ・ポリシは、マークアップ言語であるXMLで記述され、従ってソフトウェアで柔軟に処理することが可能である。

【0017】

(チケット)

図10は、本発明の実施例1を示すチケットのデータ構成図である。

チケットは、マークアップ言語であるXMLで記述され、従ってソフトウェアで柔軟に処理することが可能である。チケットは、一つ以上の個人情報とその個人情報に関する属性情報を記述したデータと、発行元の第三者機関によってこれらのデータに施されたデジタル署名から構成される。そして、WWWサーバ30

が示すポリシに従って開示情報を制御した証明書とみなすことができる。

図10に示すチケットには、チケットID、ハンドル名（承認されているか否か）、生年月日（承認されているか否か）、性別（承認されているか否か）、所属（承認されているか否か）、有効期間（年月日時）、チケット発行者、チケット発行者連絡先、およびデジタル署名が記載されている。

### 【0018】

（1回目のやりとり）

図11は、本発明の実施例1を示す1回目のやりとりのシーケンスチャートである。

図11は、図1で前述した方法と同じ手順でやりとりが行われる。先ず、クライアントからWWWサーバに対してアクセス要求を行うと、WWWサーバはアクセス確認を行い、チケットが必要であるか否かを判断し（ステップ300）、クライアントに対してチケット要求とサーバ・ポリシを返信する。クライアントは、チケット発行サーバに対してチケット要求を行い、サーバ・ポリシを附加して送信する。チケットサーバは、チケットを生成して（ステップ100）、クライアントにそのチケットを送信する。クライアントは、受取ったチケットを保存し（ステップ200）、WWWサーバに対してチケットを附加してアクセス要求を送信する。WWWサーバは、チケットを検証し、認証・アクセス制御を行い（ステップ301）、許可するときには、クライアントに対してHTMLページを送信する。不許可のときには、エラーを送信する。

### 【0019】

（2回目以降のやりとり）

図12は、本発明の実施例1を示す2回目のやりとりのシーケンスチャートである。

図12では、チケットを発行してもらい、チケットを保存しているクライアントの動作を示している。クライアントは、WWWサーバに対して保存しているチケットを附加してアクセス要求を送信する。WWWサーバは、チケットの検証と認証・アクセス制御を行い（ステップ301）、許可のときには、HTMLページをクライアントに返信する。なお、チケットの有効期限が切れたときには、再

度、チケット発行サーバに対してチケットの発行要求を送信する。

#### 【0020】

(クライアント処理)

図13は、本発明の実施例1を示すクライアントの処理フローチャートである

図13における縦線の左側は従来技術のWWWブラウザの処理であり、右側は本発明で新たに備えられるチケット処理プラグインプログラムの処理である。

WWWブラウザによりWWWサーバへアクセス要求を行うと、アクセス対象の有効なサーバ・ポリシを持っているか否かを判断し(ステップ201)、持っている場合には、アクセス対象に利用可能な有効なチケットを持っているか否かを判断し(ステップ202)、持っている場合には、そのチケットを添付して、WWWサーバへアクセス要求を行う(ステップ203)。WWWサーバから『アクセス不可』のメッセージを受信しなければ(ステップ208)、該当するページを受信して(ステップ209)、WWWブラウザに渡し、ブラウザが画面に該当ページを表示する。

一方、アクセス対象の有効なサーバ・ポリシを持っていない場合には(ステップ201)、WWWサーバへアクセス要求を行い(ステップ204)、WWWサーバから要チケットメッセージとサーバ・ポリシを受信する(ステップ205)。また、アクセス対象に利用可能な有効なチケットを持っていない場合には(ステップ202)、チケット発行サーバに対してチケット発行要求を行い、サーバ・ポリシおよびアクセス希望ディレクトリを添付して送信する(ステップ206)。チケット発行サーバからチケットを受信すると、後の利用のためにこれを保存する(ステップ207)。そして、このチケットを添付してWWWサーバにアクセス要求を行う(ステップ203)。また、WWWサーバから、『アクセス不可』のメッセージを受信した場合には(ステップ208)、エラー処理を行う(ステップ210)。

#### 【0021】

(WWWサーバの処理)

図14は、本発明の実施例1を示すWWWサーバの処理フローチャートである

WWWクライアントからアクセス要求を受信すると、アクセス制御確認を行い、チケットが必要か否かを判断し（ステップ301）、チケットが必要な場合には、チケットが要求に添付してあるか否かを判断する（ステップ302）。添付してあれば、それが正当なチケットであるか否かを判断する（ステップ303）。正当なチケットであれば、アクセスOKであるか否かを判断、すなわちサーバ・ポリシに合致するか否かを判断し（ステップ304）、OKであれば、当該するページをクライアントに送信する（ステップ305）。

一方、アクセス制御確認で、チケットが必要でなければ（ステップ301）、当該するページをクライアントに送信する（ステップ306）。また、チケットが要求に添付していない場合には（ステップ302）、『要チケット』メッセージをクライアントに送信する（ステップ307）。また、正当なチケットでないか、あるいはアクセスOKでない場合には（ステップ303、304）、『アクセス不可』のメッセージをクライアントに送信する（ステップ308）。

### 【0022】

（チケット発行サーバの処理）

図15は、本発明の実施例1を示すチケット発行サーバの処理フローチャートである。

WWWクライアントからのチケット発行要求を受信すると、チケット発行サーバは、サーバ・ポリシ、アクセス希望ディレクトリを受信し（ステップ101）、サーバ・ポリシを解析して、希望ディレクトリにアクセスするために必要な個人情報、承認の必要性、開示の必要性を調べる（ステップ102）。個人情報データベースにアクセスし、必要な情報を取得する（ステップ103）。取得した情報に基づいてチケットを作成する（ステップ100）。そのチケットをクライアントに送信する。

### 【0023】

（実施例2）

（チケット）

図16は、本発明の実施例2を示すチケットのデータ構成図である。

実施例2の特徴は、①チケットの内容全体がWWWサーバの公開鍵で暗号化されていること、②チケットには、WWWサーバとクライアントで共有するセッション鍵が記載されていること、③チケット発行サーバはクライアントにセッション鍵を送信すること、④クライアントは受信したセッション鍵で認証子を作成すること、⑤WWWサーバに対して暗号化チケットと認証子を添付してアクセスを要求すること、⑥WWWサーバは、チケットからセッション鍵を取り出し、その鍵で認証子を復号化し、確かに本人から要求されたか否かを検証すること、を有しており、実施例1よりもさらに厳しい検証を受けてアクセスが許可されることになる。

図16に示すように、チケットの内容は実施例1の場合と同じ内容に、セッション鍵が追加されている。すなわち、WWWサーバとクライアントで共有するセッション鍵を、チケット発行サーバが生成して、利用するWWWサーバの公開鍵でチケットの内容を暗号化する。従って、クライアントには、暗号化されたチケットが送信される。

#### 【0024】

(認証子)

図17は、本発明の実施例2を示す認証子の作成および検証の方法の説明図である。

実施例2では、認証子が必要となるが、これはチケットの正当な保持者であることを証明するためのものである。

実施例2では、実施例1の手続きに、チケットの不正利用防止機構を追加した手続きを採用する。チケット不正利用防止機構は、公知のKerberosの技術を利用する。すなわち、実施例1の方法を採用した場合、悪意を持った者がクライアントのやりとりを監視して、後で同一データをWWWサーバに送信すれば、正当なクライアントになりすましてアクセスが可能になってしまふおそれがある。これを防止するために、Kerberosの技術では、一般にアクセスを要求する時刻をセッション鍵で暗号化する方法を採用している。

#### 【0025】

図17に示すように、認証子の作成は、要求時刻（例えば、2000年9月1日13:1

3) 60をセッション鍵で暗号化して、認証子を作成する。

次に、WWWサーバによる認証子の検証は、送信された認証子を同じセッション鍵で復号化する。これにより、要求時刻：(2000年9月1日13:13) 62が得られる。WWWサーバは、要求時刻が現在の時刻から許容範囲内にあるか否か、および、許容範囲内の場合、その範囲内に同じ時刻の認証子を受信していないかを確認することにより、不正に他人が同じ認証子を再送することを防止することができる。もし、正当なクライアントが送信した認証子を利用して、不正にアクセスする者がWWWサーバにアクセス要求をしても、その認証子は以前に正当なクライアントがアクセスした時刻であるため、許容範囲より外れている場合は、検証の結果、不正アクセスと判断される。

また、WWWサーバは、許容時刻の範囲だけ過去の認証子を記憶しておけばよい。

認証子を作成したり、検証できる者は、セッション鍵を知っている者、つまり正当なクライアントとWWWサーバであり、それ以外の者は認証子を作成したり、検証したりすることは不可能である。

### 【0026】

(1回目のやりとり)

図18は、本発明の実施例2を示す1回目のやりとりのシーケンスチャートである。

クライアントはWWWサーバに対してアクセス要求を行うと、WWWサーバはアクセスを確認し、要チケットであるか否かを判断する(ステップ300A)。WWWサーバはクライアントにチケット要求とサーバ・ポリシを添付して返送する。クライアントはチケット発行サーバに対して、チケット要求およびサーバ・ポリシを送信する。ここまででは、実施例1と同じである。チケット発行サーバは、セッション鍵を生成するとともに、チケットを生成する(ステップ100A)。チケット発行サーバは、生成したチケットとセッション鍵をクライアントに送信する。クライアントは、セッション鍵とチケットを保存し、セッション鍵で認証子を作成する(ステップ200A)。そして、WWWサーバに対して、チケットと認証子を添付してアクセス要求を行う。WWWサーバは、認証子とチケット

検証を行うとともに、認証・アクセス制御を行う（ステップ301A）。検証の結果、許可するときには、クライアントにHTMLページを送信する。

### 【0027】

#### (クライアントの処理)

図19は、本発明の実施例2を示すクライアントの処理フローチャートである

WWWブラウザにより、WWWサーバへアクセス要求を行うことで、アクセス対象の有効なサーバ・ポリシを持っているか否かを判断し（ステップ201）、持っている場合には、アクセス対象に利用可能な有効なチケットを持っているか否かを判断する（ステップ202）。両方とも持っている場合には、時刻をセッション鍵で暗号化して認証子を作成する（ステップ202A）。そして、チケットと認証子を添付してWWWサーバにアクセス要求を行う（ステップ203A）。WWWサーバから『アクセス不可』のメッセージを受信しない場合には（ステップ208）、当該するページを受信する（ステップ209）。このページをWWWブラウザに渡すことにより、ブラウザは画面にこのページを表示する。

一方、アクセス対象の有効なサーバ・ポリシを持っていない場合には（ステップ201）、WWWサーバにアクセス要求を行い（ステップ204）、WWWサーバから要チケットメッセージとサーバ・ポリシを受信する（ステップ205）。また、アクセス対象に利用可能な有効なチケットを持っていない場合には（ステップ202）、チケット発行要求を行い、サーバ・ポリシおよびアクセス希望ディレクトリをチケット発行サーバに送信する（ステップ206）。チケット発行サーバからチケット、セッション鍵を受信して、後の利用のためにこれらを保存する（ステップ207A）。そして、時刻をセッション鍵で暗号化して認証子を作成し（ステップ202A）、チケットと認証子を添付してWWWサーバにアクセス要求を行う（ステップ203A）。『アクセス不可』のメッセージを受信した場合には（ステップ208）、エラー処理を行う（ステップ210）。

### 【0028】

#### (WWWサーバの処理)

図20は、本発明の実施例2を示すWWWサーバの処理フローチャートである

WWWクライアントからのアクセス要求を受信すると、アクセス制御確認を行い、要チケットであるか否かを判断する（ステップ301）。要チケットであれば、チケット、認証子が要求に添付してあるか否かを判断する（ステップ302）。添付してあれば、正当なチケットであるか否かを判断する（ステップ303）。正当なチケットであれば、認証子の検証はOKか否かを判断する（ステップ3031）。検証が許可範囲内にあれば、アクセスOKか否かを判断、すなわちサーバ・ポリシに合致するか否かを判断し（ステップ304）、OKであれば、該当するページをクライアントに送信する（ステップ305）。

一方、要チケットでない場合には（ステップ301）、該当するページをクライアントに送信する（ステップ306）。また、チケット、認証子が要求に添付していない場合には（ステップ302A）、『要チケット』メッセージをクライアントに送信する（ステップ307）。また、正当なチケットでないか、あるいは認証子の検証がNOであるか、あるいはアクセスOKでないか（サーバ・ポリシに不一致）のいずれかであれば（ステップ303, 3031, 304）、『アクセス不可』のメッセージをクライアントに送信する（ステップ308）。

#### 【0029】

（チケット発行サーバの処理）

図21は、本発明の実施例2を示すチケット発行サーバの処理フローチャートである。

WWWクライアントからのチケット発行要求を受信すると、チケット発行サーバは、チケット発行要求に添付されているサーバ・ポリシ、アクセス希望ディレクトリを受信する（ステップ101）。次に、サーバは、サーバ・ポリシを解析し、希望ディレクトリにアクセスするために必要な個人の情報、承認の必要性、開示の必要性を調べる（ステップ102）。次に、個人情報データベースにアクセスして、必要な情報を取得し（ステップ103）、セッション鍵を作成し（ステップ104）、チケットを作成する（ステップ100）。作成したチケットと、セッション鍵をクライアントに送信する。

#### 【0030】

## (実施例2の詳細フロー)

図22は、本発明の実施例2を示す認証またはアクセス管理方法の詳細フローチャートである。

チケット発行サーバは、クライアントからチケット発行要求を受けると、セッション鍵を生成し、チケットを発行して、生成したセッション鍵を記載した後、そのチケットをWWWサーバの公開鍵で暗号化する（ステップ100B）。そして、クライアントに対して、暗号化したチケットと生成されたセッション鍵を送信する。

クライアントは、受信したチケットおよびセッション鍵を保存し、現在の時刻をセッション鍵で暗号化して認証子を作成する（ステップ200B）。そして、WWWサーバに対して、暗号化したチケットおよび作成した認証子を添付してアクセス要求を行う。

WWWサーバは、暗号化したチケットを復号化する。そして、セッション鍵を取り出す。このセッション鍵で認証子を復号化して時刻を取り出す。次にその時刻を検証する。受信時刻の許容範囲内にあれば、確かにクライアント本人であることを判別する。また、チケット・サーバ・ポリシを検証し、合致していれば、アクセスOKと判断する。

アクセスOKの場合には、クライアントに対してHTMLページを送信する。

もし、アクセスNOの場合には、アクセス不可を送信することにより、クライアントはエラー処理を行う。

## 【0031】

## (プログラム記録媒体)

図13（実施例1のWWWブラウザの処理）、図14（同WWWサーバの処理）、図15（同チケット発行サーバの処理）、図19（実施例2のクライアントの処理）、図20（同WWWサーバの処理）、図21（同チケット発行サーバの処理）、および図22（同実施例2の処理手順）の各処理ステップをプログラムに変換し、そのプログラムをCD-ROMなどの記録媒体に格納しておく。これにより、インターネットに接続された任意の端末のパソコンに実装し、プログラムをインストールするか、あるいはネットワークを介して他のパソコンにダウン

ロードして、プログラムを実施すれば、本発明を容易に実現することができる。

【0032】

【発明の効果】

以上説明したように、本発明によれば、信頼のある個人情報を基にアクセス管理が可能になるとともに、個人情報を秘匿しながらの身元保証が可能となる。これにより、匿名の投稿が可能になり、信頼できるハンドル名の使用が可能となる。また、女性だけのアクセス許可や、年令制限を有するアクセス許可が可能となる。

【図面の簡単な説明】

【図1】

本発明の原理（アクセス制御の解決手段1）を示す説明図である。

【図2】

本発明の原理（不適正書き込みの解決手段1）を示す説明図である。

【図3】

本発明の原理（性別によるアクセス管理の解決手段2）を示す説明図である。

【図4】

本発明の実施例1を示すネットワークの構成図である。

【図5】

図4におけるクライアントの詳細構成図である。

【図6】

図4におけるチケット発行サーバの詳細構成図である。

【図7】

図4におけるWWWサーバの詳細構成図である。

【図8】

本発明の実施例1を示す個人情報データベースのデータ構成図である。

【図9】

本発明の実施例1を示すサーバ・ポリシのデータ構成図である。

【図10】

本発明の実施例1を示すチケットのデータ構成図である。

【図11】

本発明の実施例1を示す1回目のやりとりのシーケンスチャートである。

【図12】

同2回目以降のやりとりのシーケンスチャートである。

【図13】

本発明の実施例1を示すクライアントの処理フローチャートである。

【図14】

本発明の実施例1を示すWWWサーバの処理フローチャートである。

【図15】

本発明の実施例1を示すチケット発行サーバの処理フローチャートである。

【図16】

本発明の実施例2を示すチケットのデータ構成図である。

【図17】

本発明の実施例2を示す認証子の作成および検証の説明図である。

【図18】

本発明の実施例2を示す1回目のやりとりのシーケンスチャートである。

【図19】

本発明の実施例2を示すクライアントの処理フローチャートである。

【図20】

本発明の実施例2を示すWWWサーバの処理フローチャートである。

【図21】

本発明の実施例2を示すチケット発行サーバの処理フローチャートである。

【図22】

本発明の実施例2を示す詳細処理のフローチャートである。

【符号の説明】

1 0…信頼できる第三者機関A B C、 2 0…ユーザ、 3 0…WWWサーバ、

1 1…個人情報データベース、 1 2…チケット、 3 1…サーバ・ポリシ、

4 0…ネットワーク、 5 0…インターネット、 1 4, 2 4, 3 5…C P U、

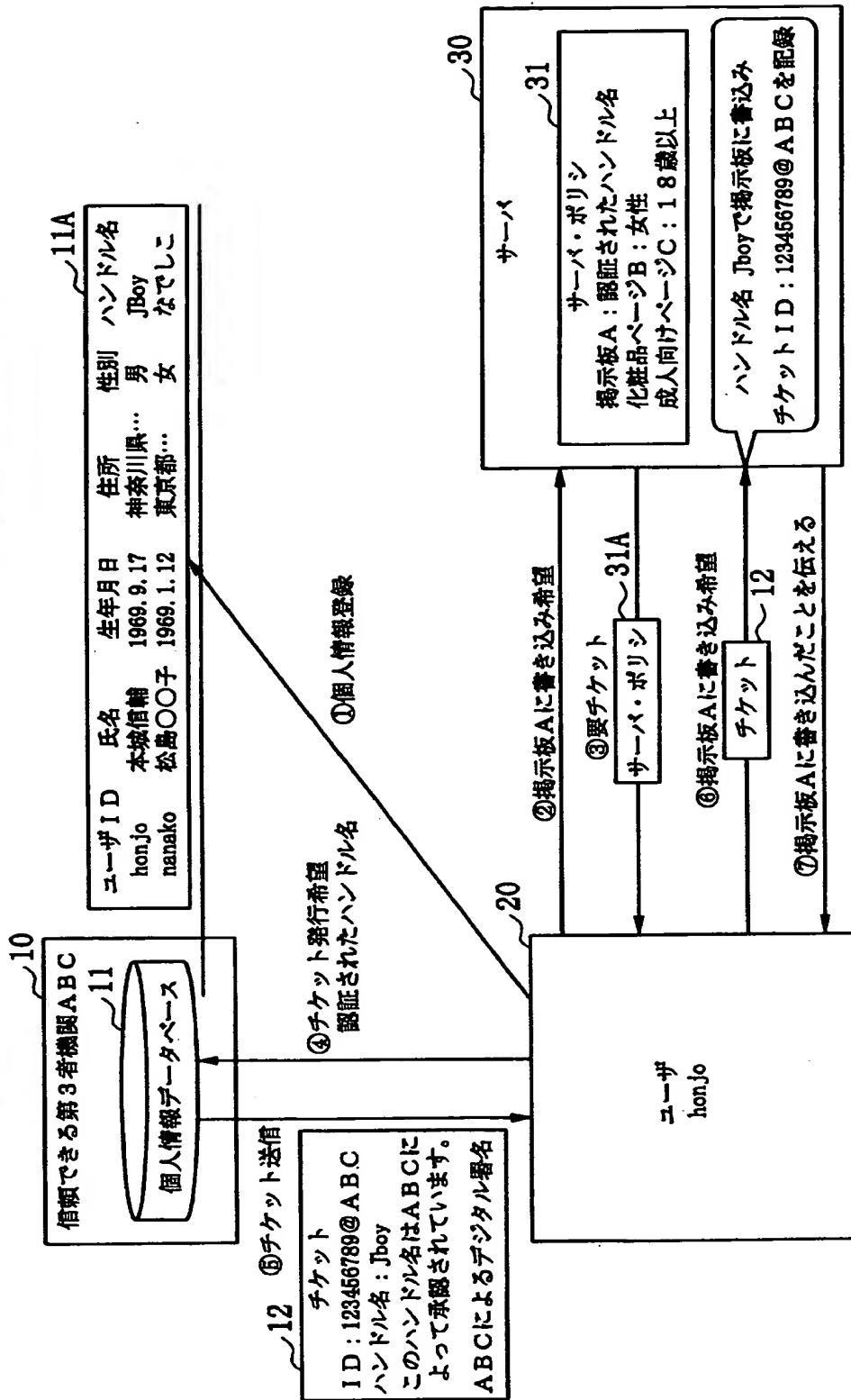
1 3…チケット発行プログラム、 2 5, 3 6…ハードディスク、

12, 23, 34…オペレーティングシステム、  
15, 26, 37…表示装置、16, 27, 38…入力装置、  
17, 28, 39…ネットワークインターフェース、  
22…WWWブラウザプログラム、33…WWWサーバプログラム、  
21…チケット処理プラグインプログラム、70…調停者、  
32…チケット認証・アクセス管理プログラム、60…要求時刻、  
61…認証子、62…復号化された時刻。

【書類名】 図面

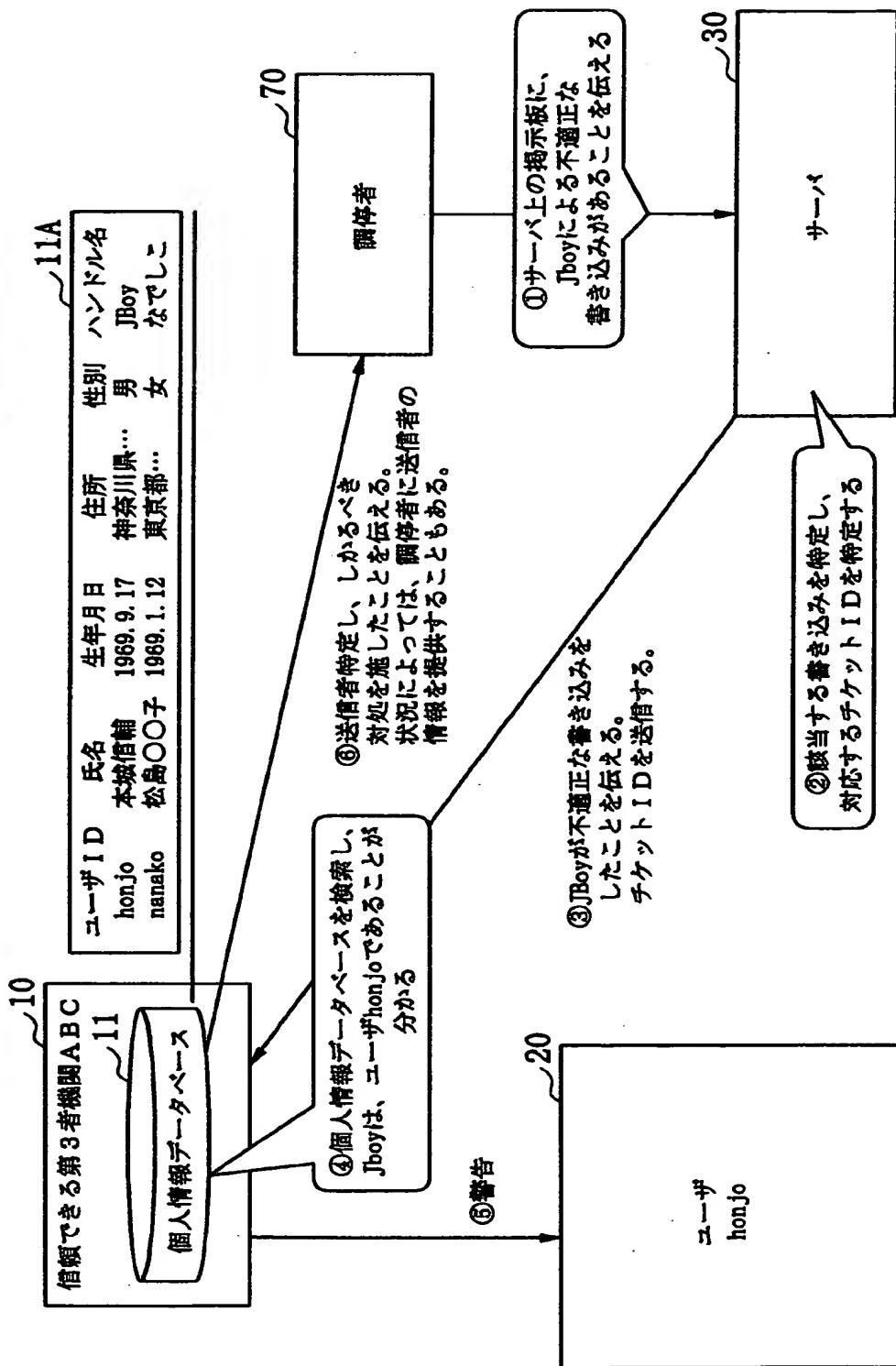
【図1】

## 課題の解決手段1（承認されたハンドル名によるアクセス制御）



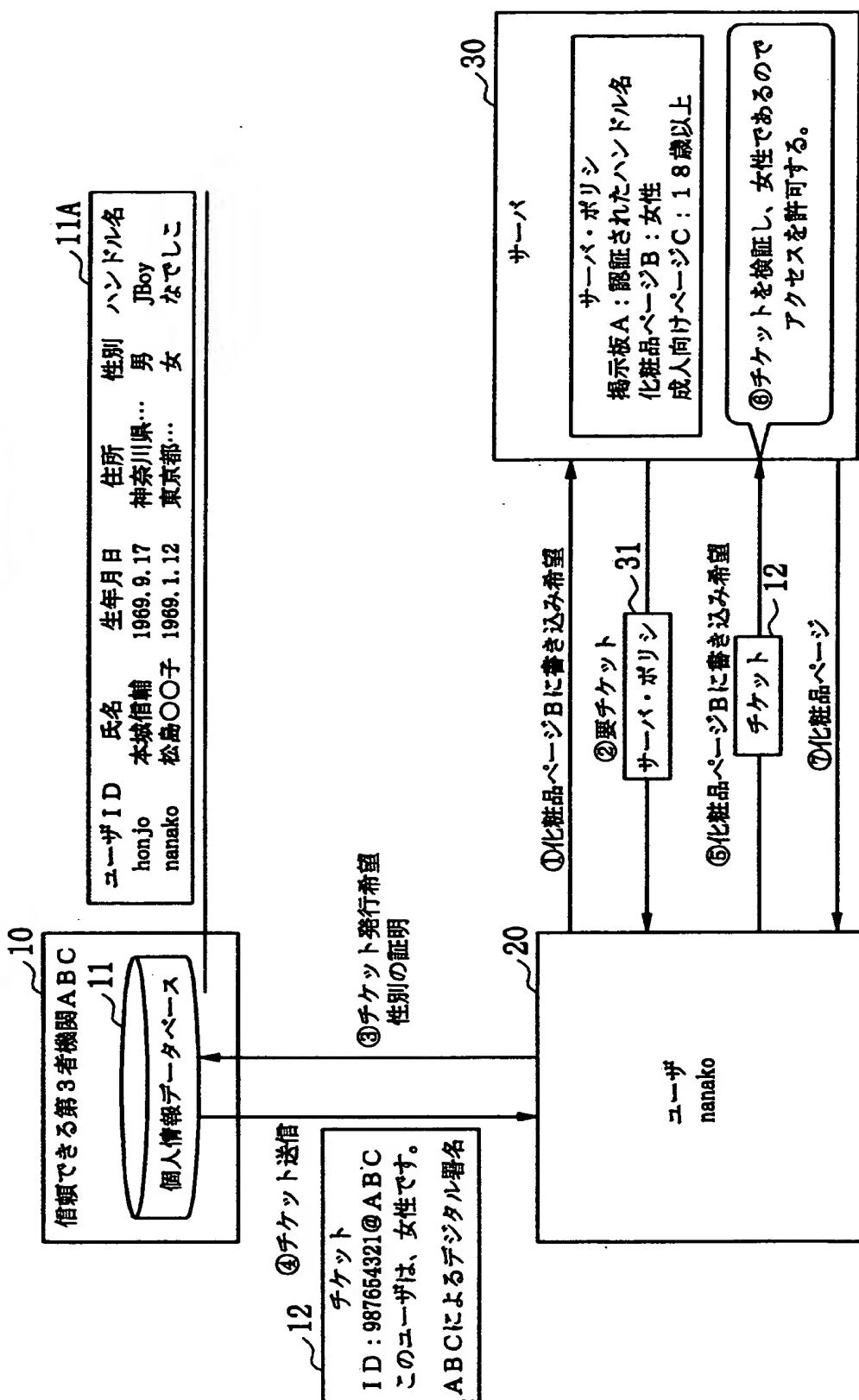
## 課題の解決手段1（承認されたハンドル名によるアクセス制御）

【図2】



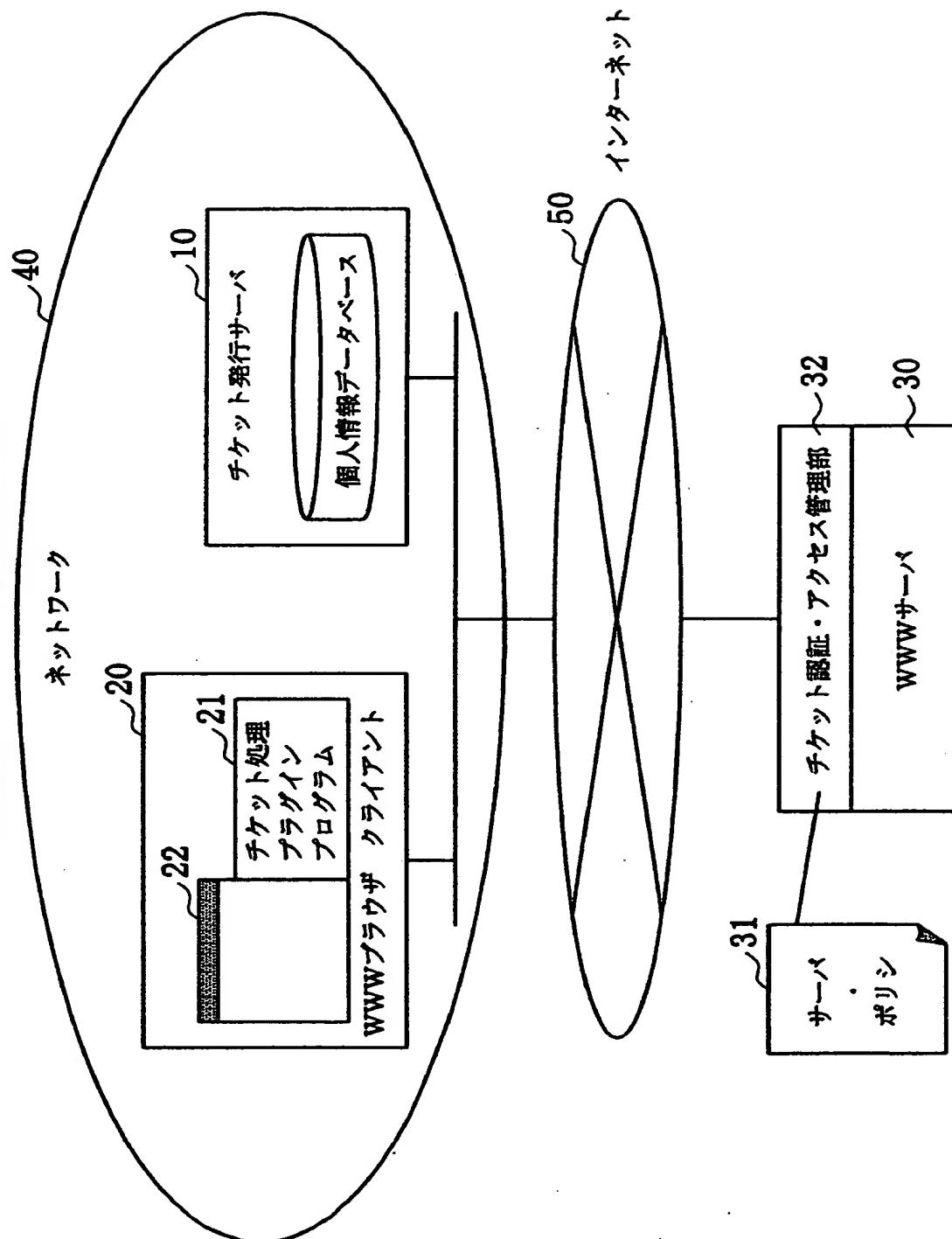
【図3】

## 課題の解決手段2（性別によるアクセス管理）

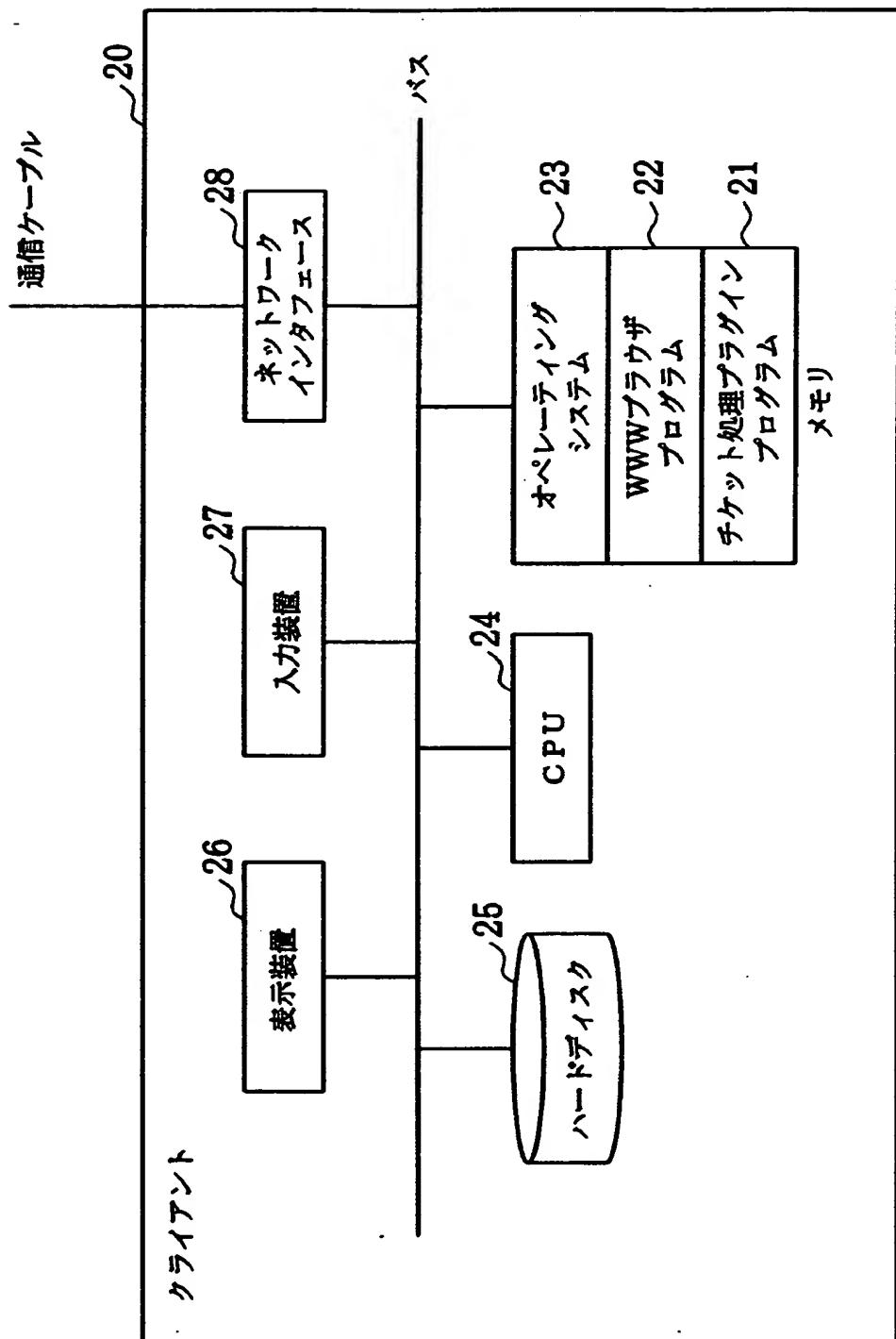


実施例1：ネットワークの構成

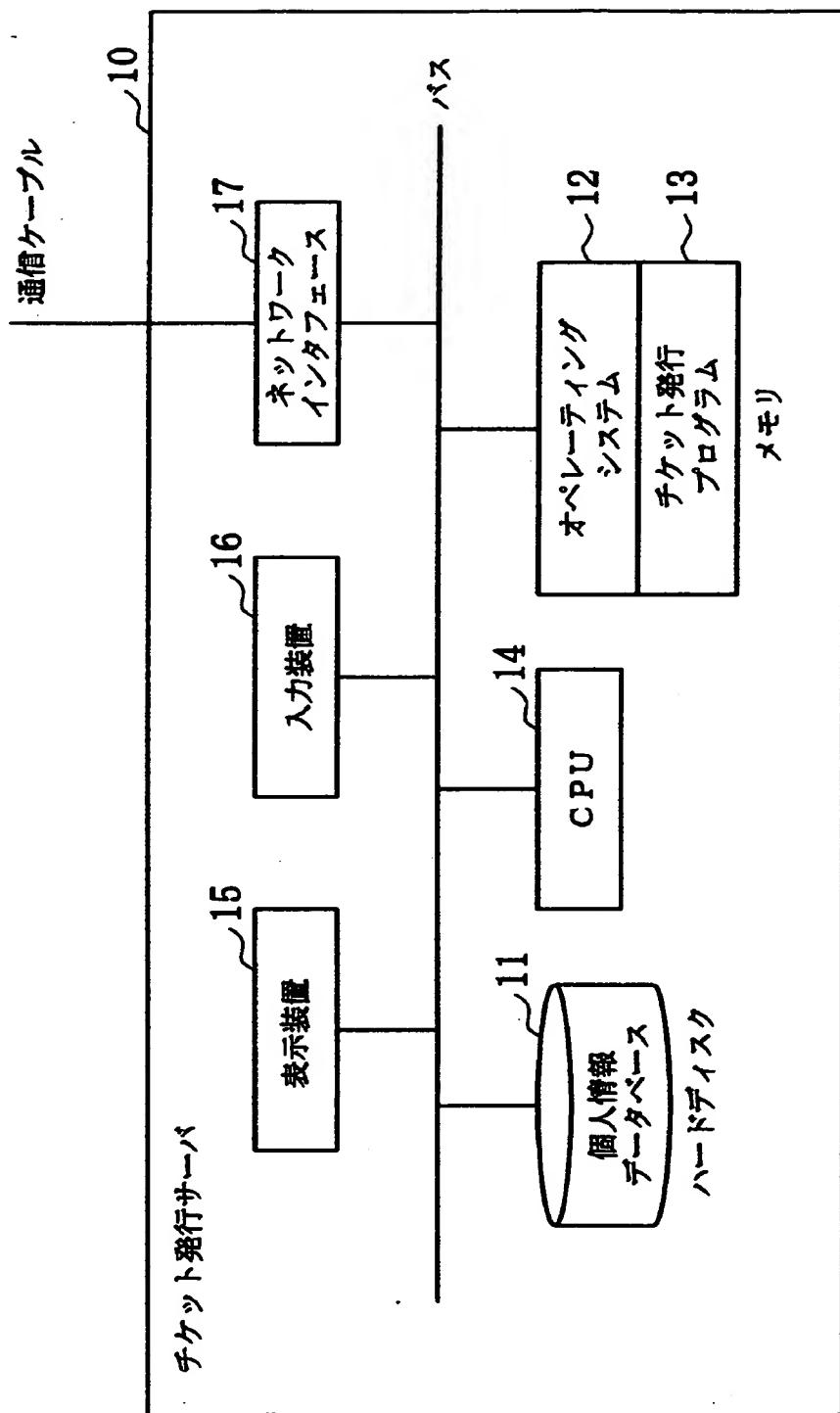
【図4】



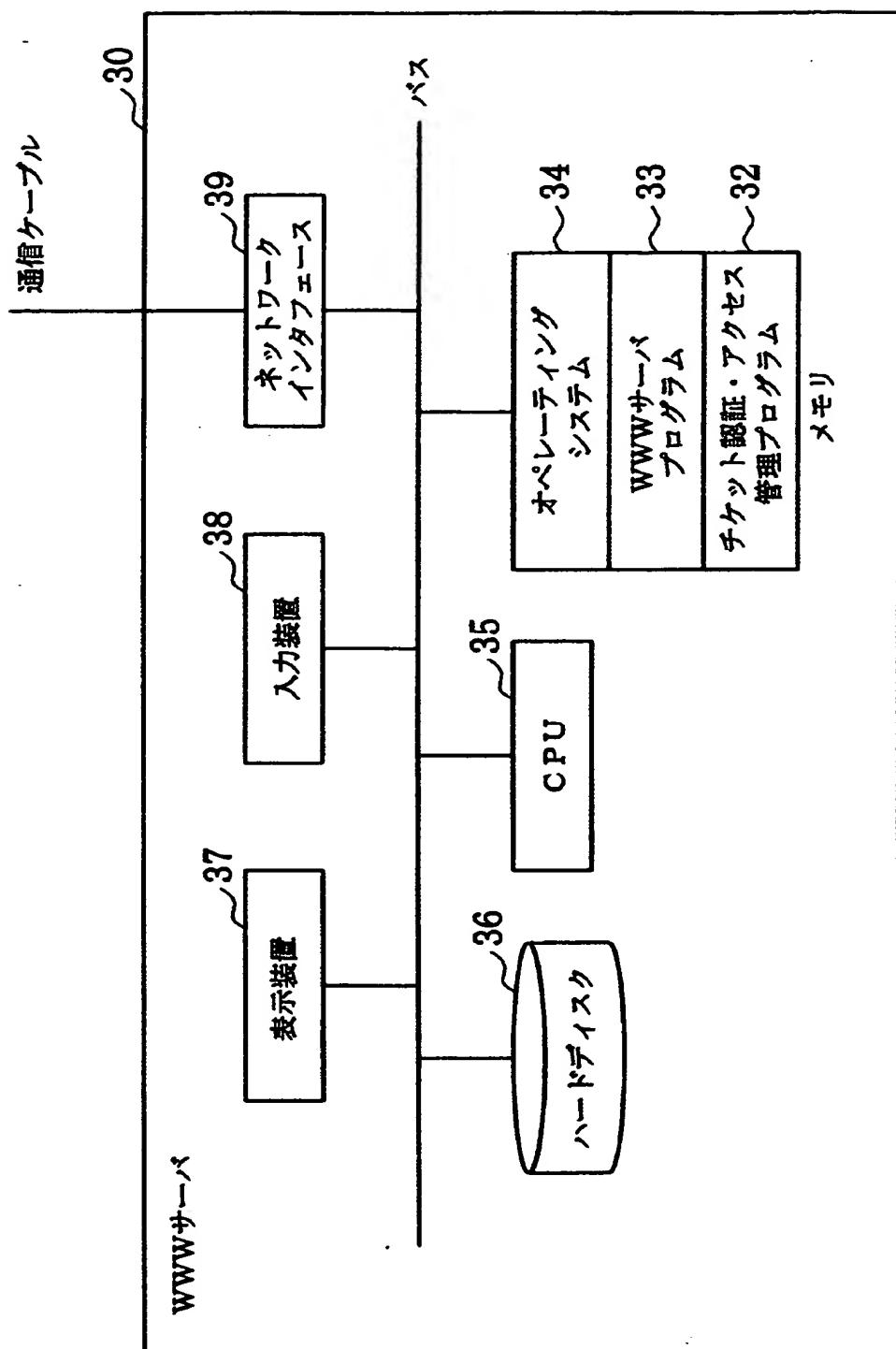
【図5】



【図6】



【図7】



## 実施例1：個人情報データベース

【図8】

ユーザID	氏名	連絡先	生年月日	性別	ハンドル名	所属	メールアドレス
yamada	山田花子 Hanako Yamada	大阪府… 1-21-31	1976.1.1	女	花子	総務部	abc@def.co.jp
ichiro	鈴木一郎 Ichiro Suzuki	愛知県… 1-2-3	1980.12.1	男	イチロー	技術部	pqr@xyz.co.jp

実施例1：サーバ・ポリシ

【図9】

サーバ：www.a b c. com  
ディレクトリ：/c g i - b i n/b b s /

サービス：掲示板

必要な情報：ハンドル名、要承認、開示

必要な情報：氏名、要承認、非開示

必要な情報：連絡先、要承認、非開示

ディレクトリ：/w o m e n /

サービス：女性専用ページ

必要な情報：ハンドル名、要承認、開示

必要な情報：性別＝“女”，要承認、開示

ディレクトリ：/v i o l e n c e /

サービス：映画情報ページ（暴力シーン・性的なシーンあり）

必要な情報：年齢≥“18”，要承認、開示

有効期間：2000年5月1日12：00～2000年10月2日12：00

【図10】

実施例1：チケット

チケットID: 1234456789@xyz.com

ハンドル名: イチロー、承認  
生年月日: 1960年12月1日、承認  
性別: 男、承認  
所属: 技術部、未承認

有効期間: 2000年9月1日12:00-2000年9月2日12:00

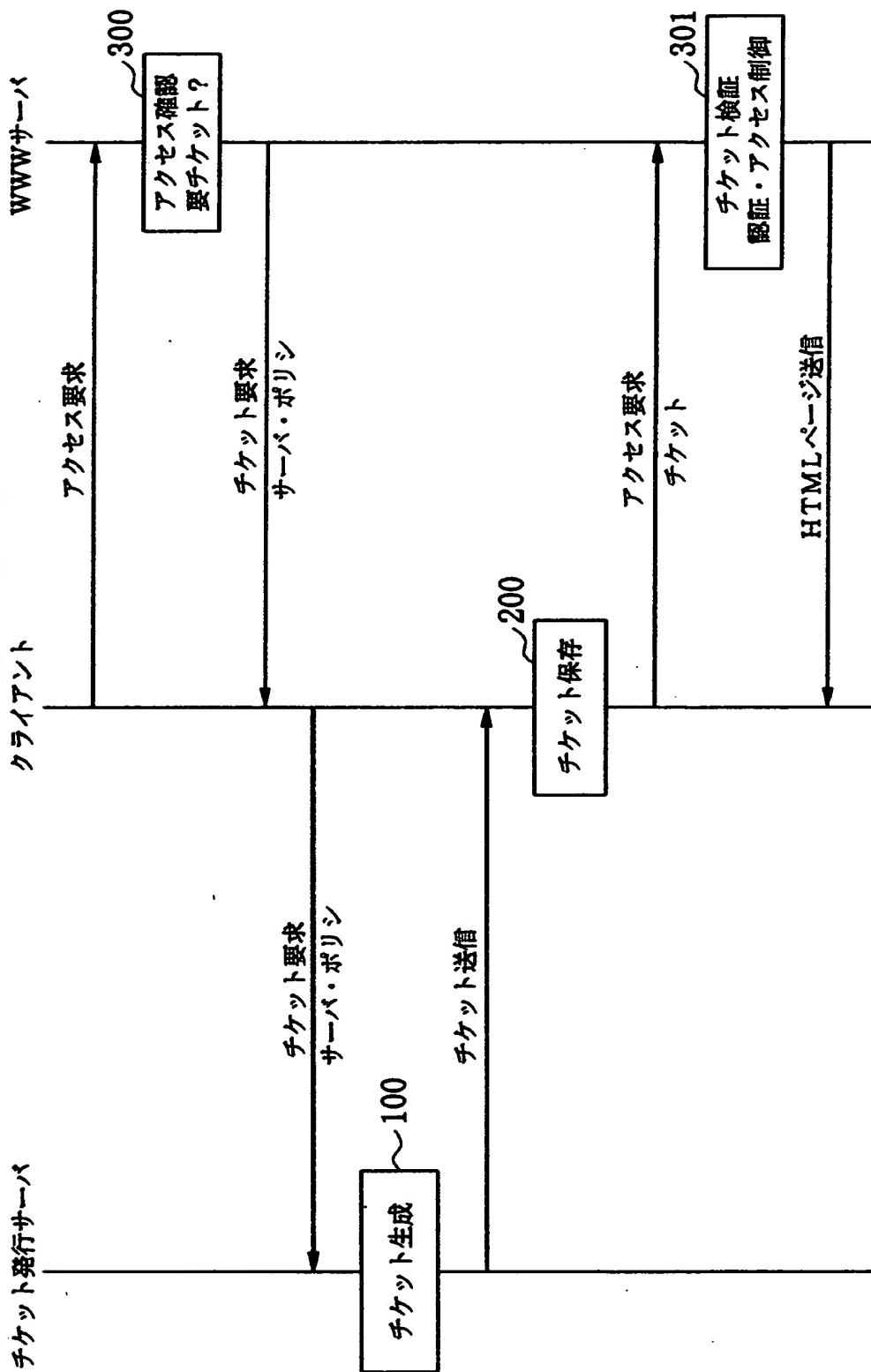
チケット発行者: XYZ

チケット発行者連絡先: admin@xyz.com

デジタル署名: -----

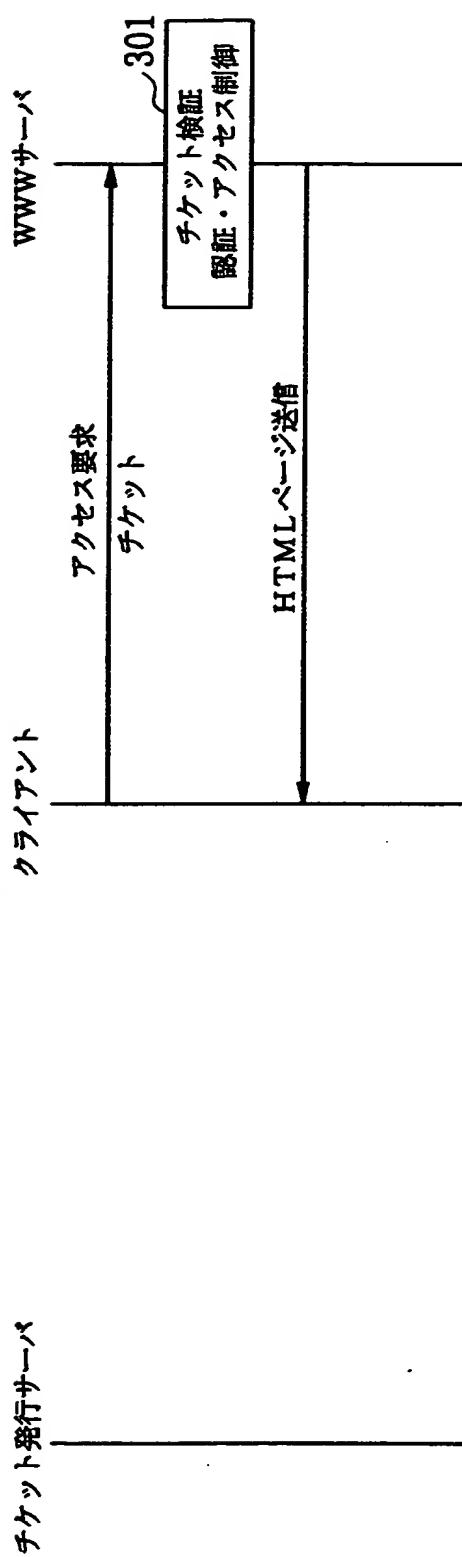
実施例1：1回目のやりとり

【図1.1】

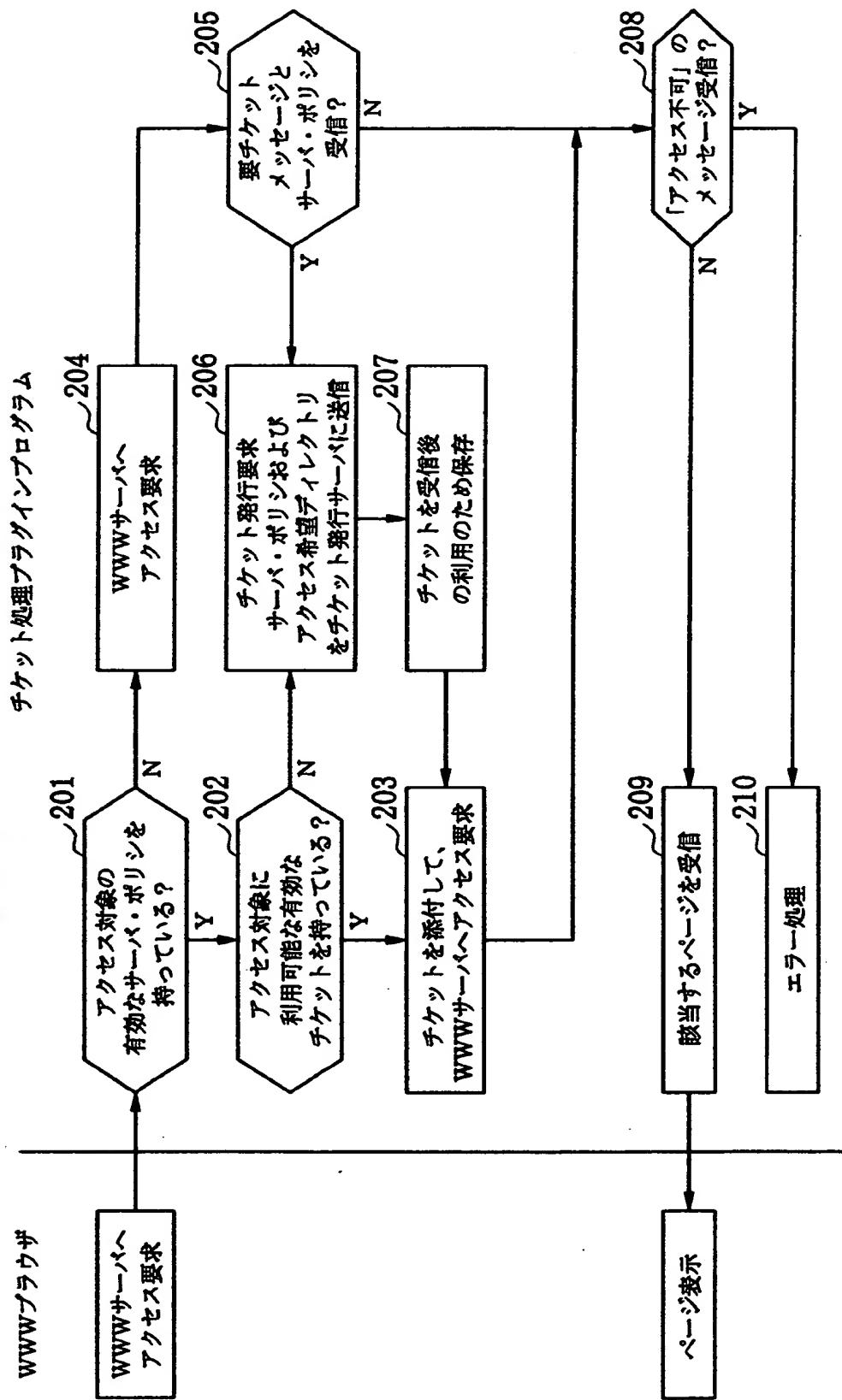


【図12】

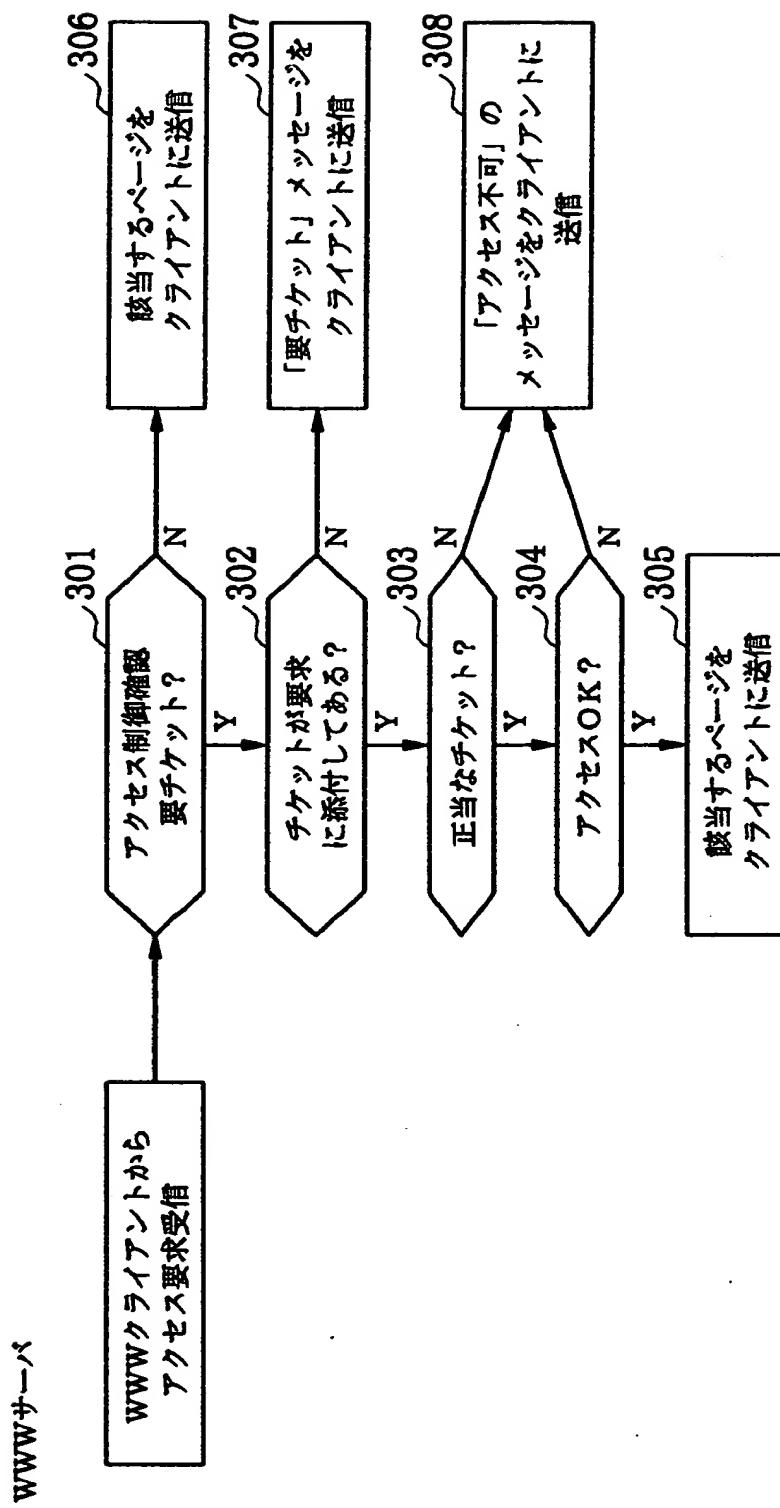
実施例1：2回目以降のやりとり



【図13】

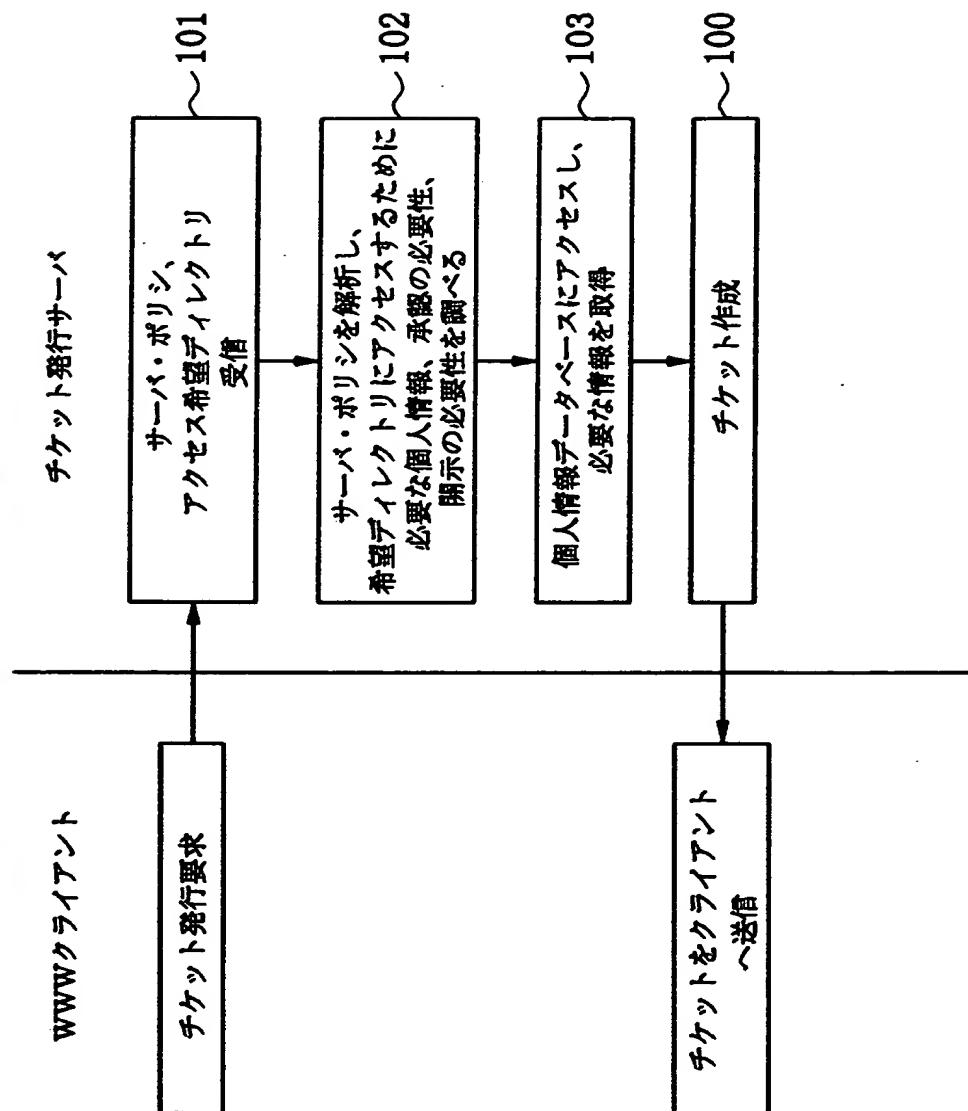
実施例1：クライアントの処理

【図14】

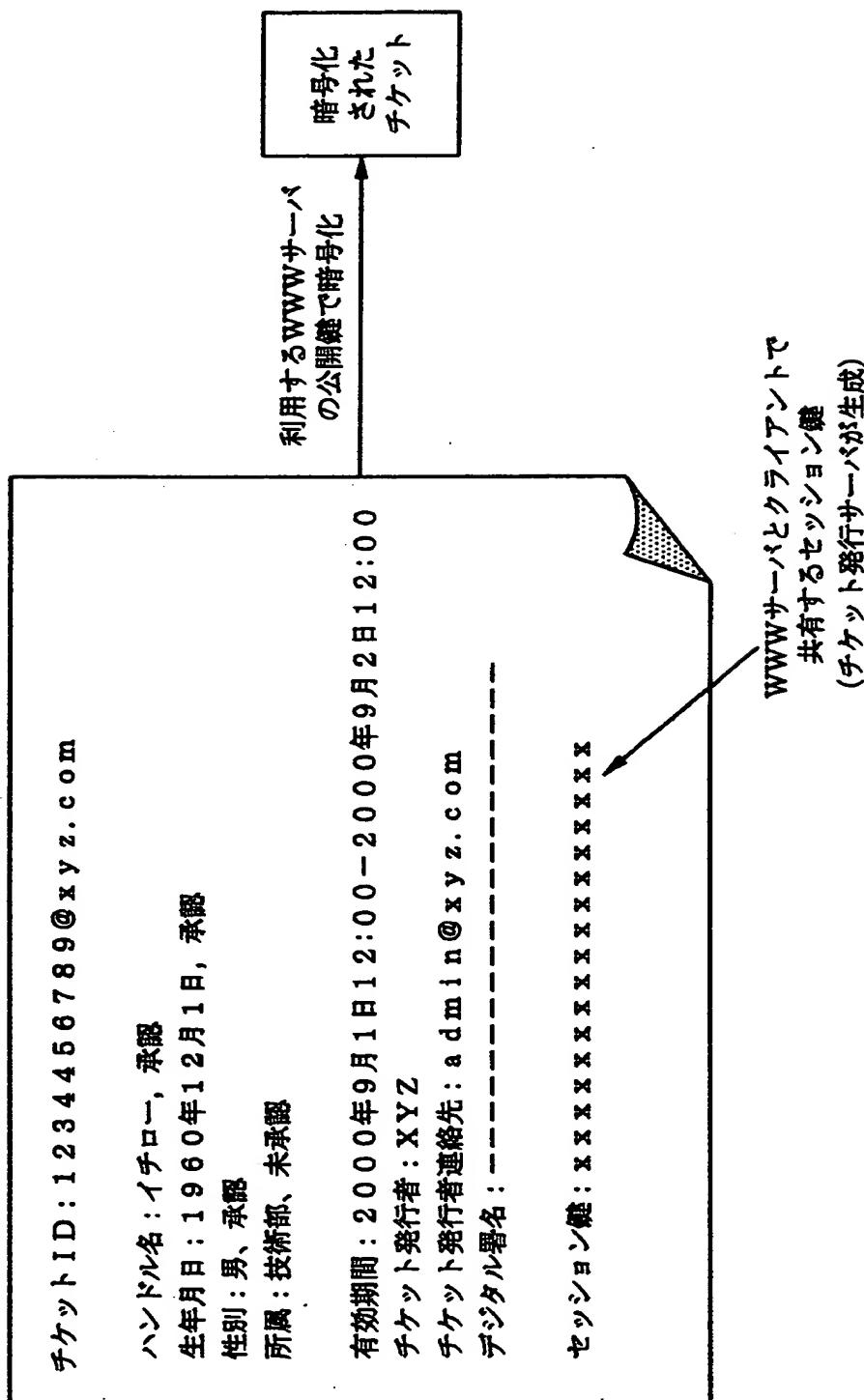
実施例1：WWWサーバの処理

実施例1：チケット発行サーバーの処理

【図15】



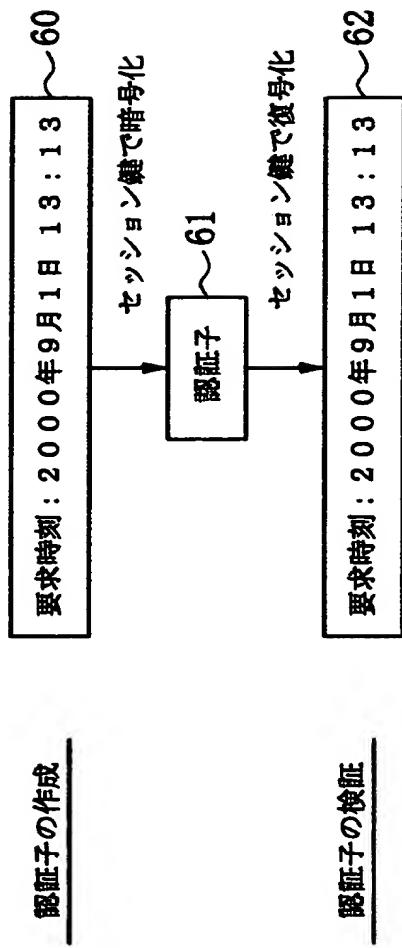
【図16】

実施例2：チケット

【図17】

実施例2：認証子（チケットの正当な保持者であることを証明するためのもの）

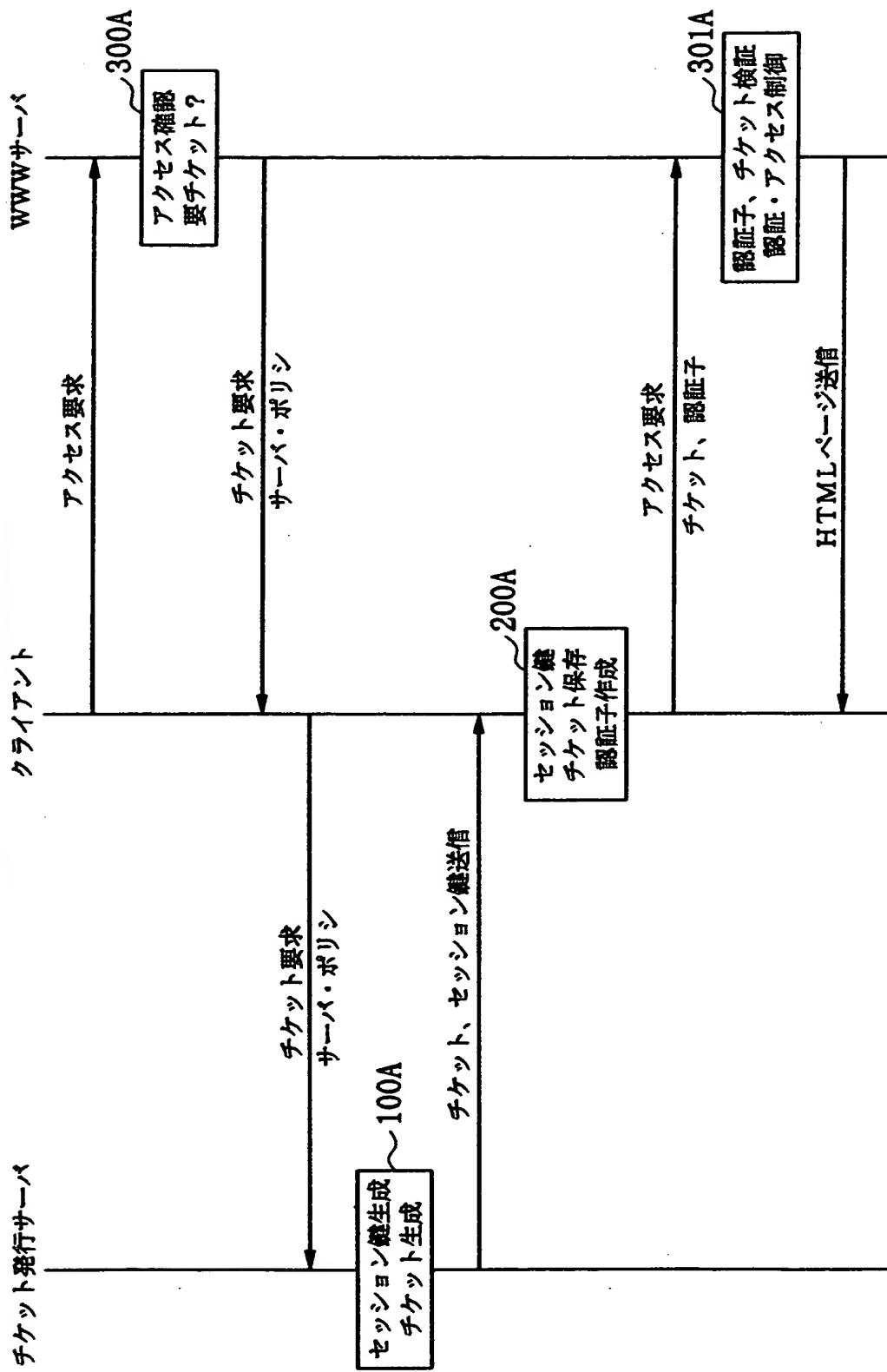
---



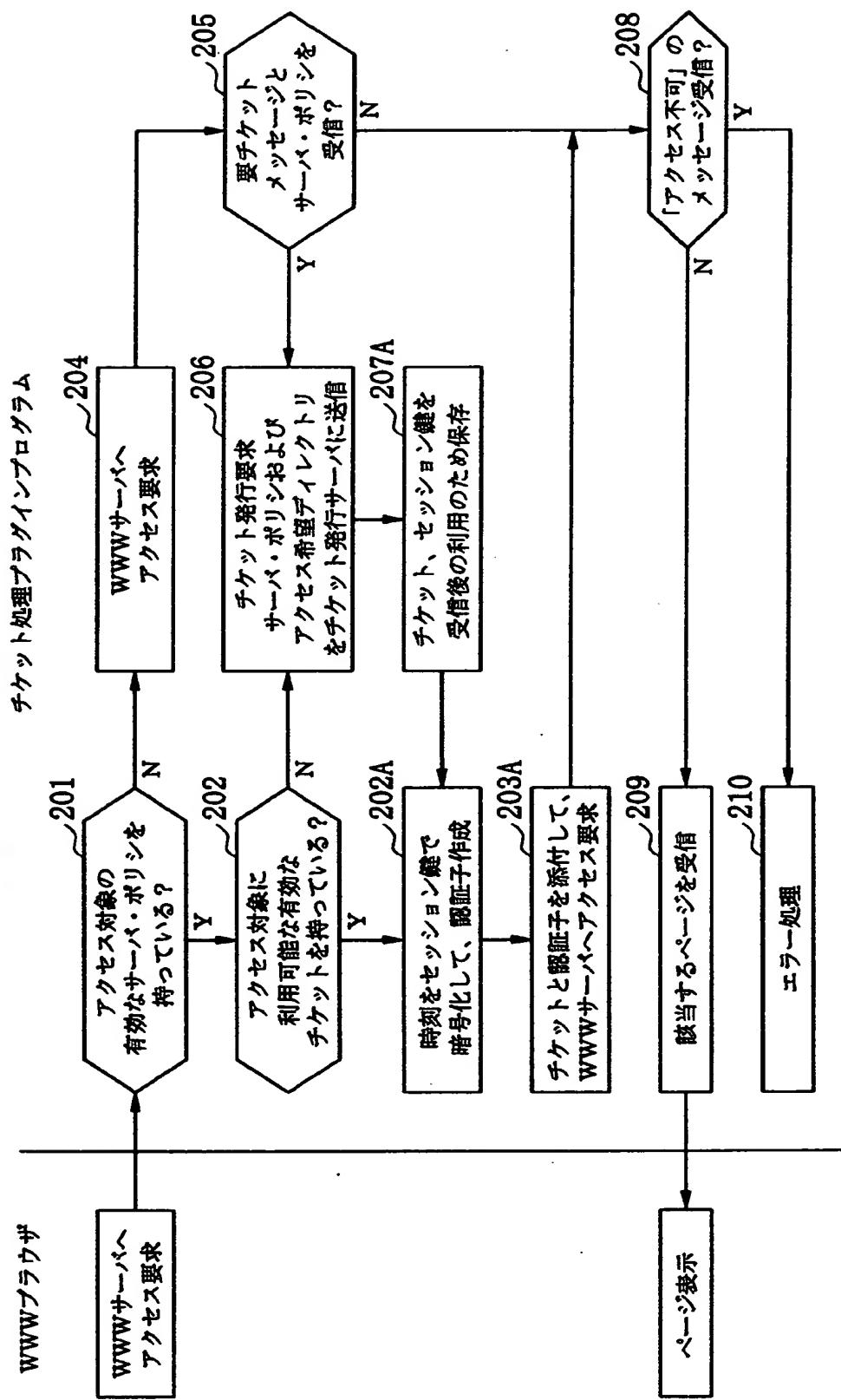
要求時刻が現在の時刻から許容範囲内にあるかどうか確認  
(不正に他人が同じ認証子を再送するのを防ぐ)

注意) 認証子を作ったり検証できる人＝セッション鍵を知っている人  
つまり、クライアント（チケット発行サーバにセッション鍵を教えてもらう）  
とWWWサーバ（チケットを復号化して、セッション鍵を取り出せる）  
それ以外の人は、認証子を作ったり、検証したりすることはできない

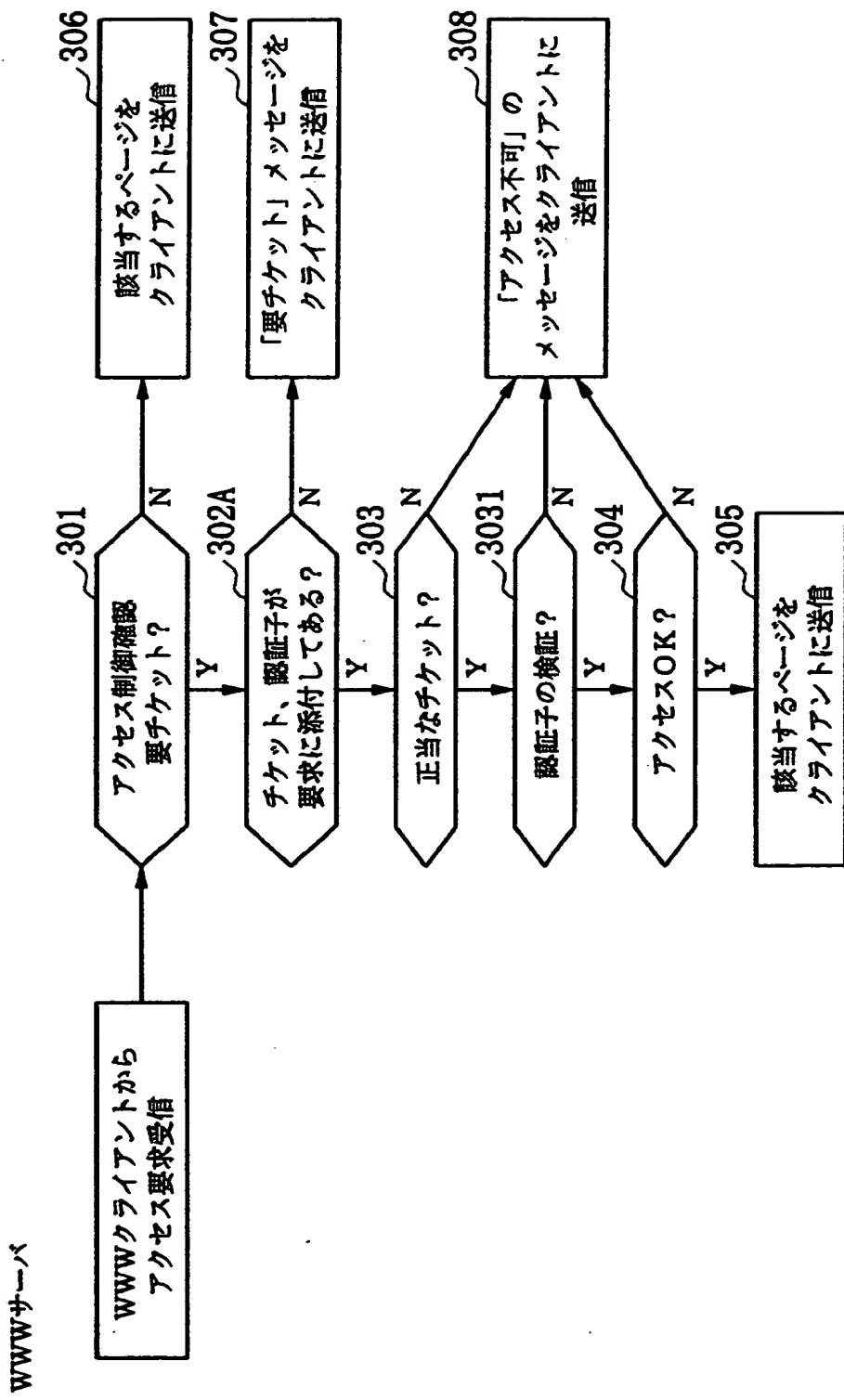
【図18】

実施例2：1回目のやりとり

【図19】

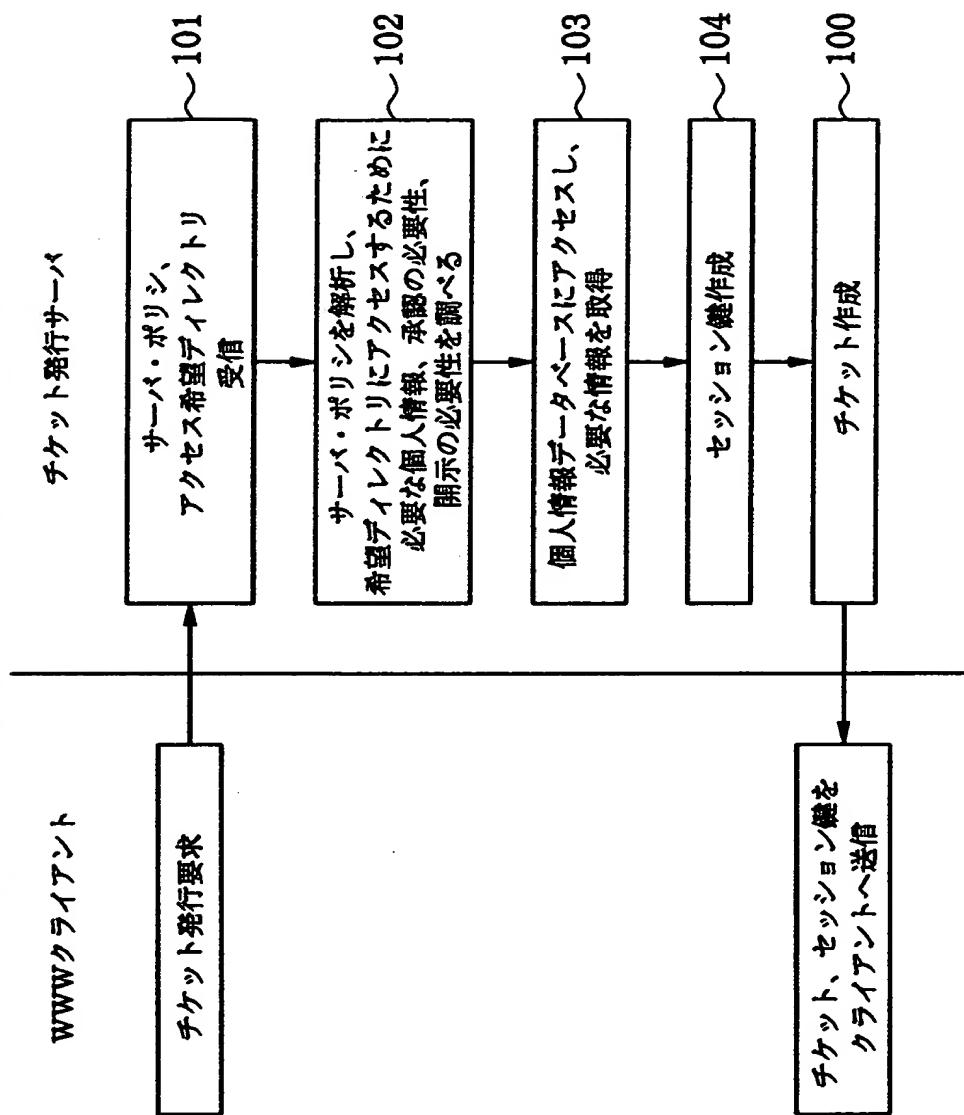
実施例2：クライアントの処理

【図20】

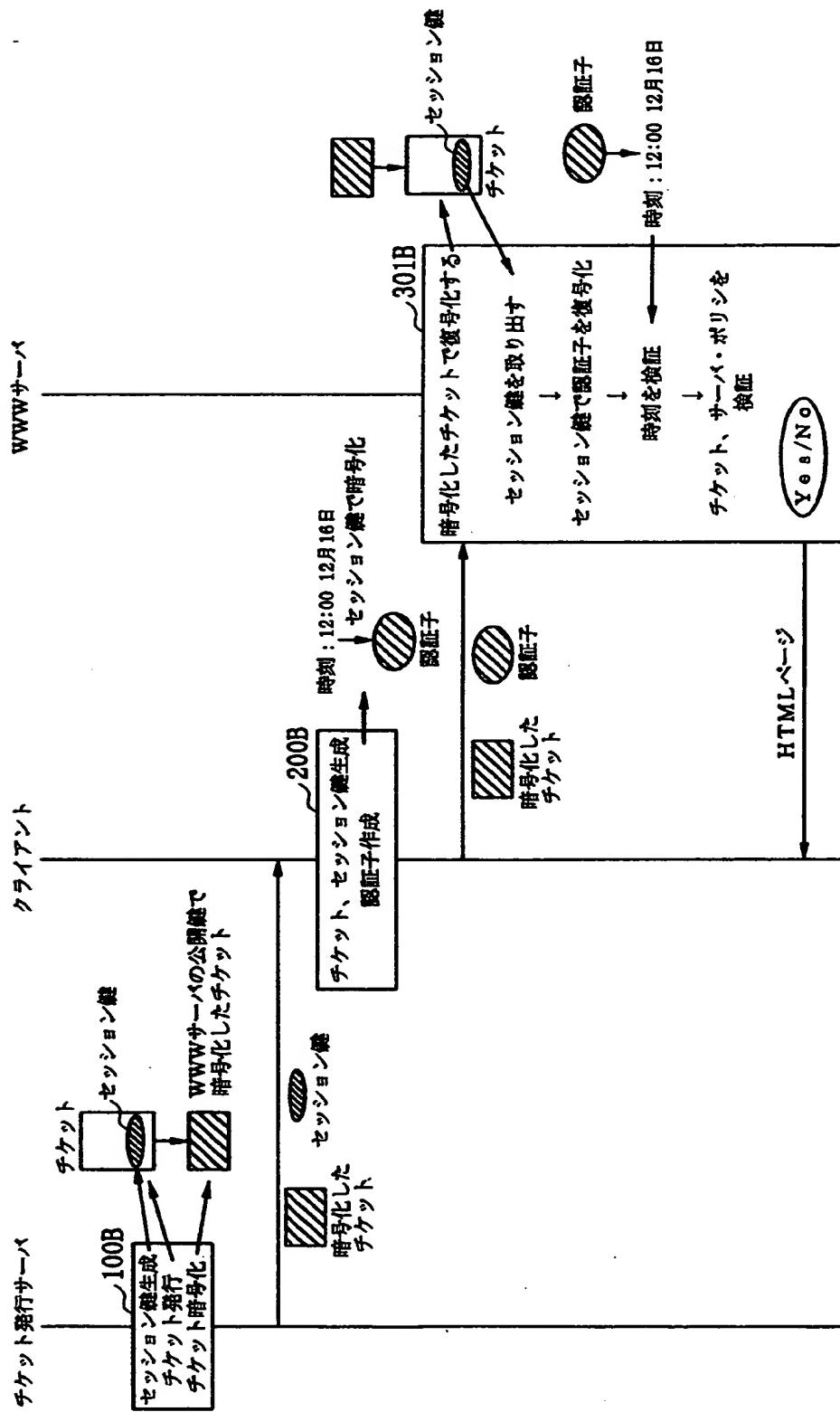
実施例2：WWWサーバの処理

実施例2：チケット発行サーバーの処理

【図21】



【図22】



【書類名】 要約書

【要約】

【課題】 信頼のある個人情報を基にアクセス管理を可能にするとともに、個人情報を秘匿しながらの身元保証を可能にする。

【解決手段】 ①ユーザ20は個人情報を第三者機関10に登録する。②③アクセス制御を行うサーバ30は、その条件を記載したサーバ・ポリシ31を設定する。サーバ・ポリシの記載内容としては、対象ディレクトリ、必要な情報、情報の開示レベル、情報の承認が必要か否かである。④ユーザ20は、第三者機関10に必要な情報を承認してもらうために、⑤チケット12を発行してもらう。⑥ユーザ20は、チケット12をサーバ30に提示、サーバ30は、チケット12の内容とサーバ・ポリシ31とを照らし合わせ、アクセス可能か否かを判断する。⑦OKの場合には、掲示板に書き込みOKをユーザ20に返送する。

【選択図】 図1

## 認定・付加情報

特許出願の番号	特願2000-320645
受付番号	50001357858
書類名	特許願
担当官	佐藤 一博 1909
作成日	平成12年11月 2日

## &lt;認定情報・付加情報&gt;

【提出日】	平成12年10月20日
【特許出願人】	
【識別番号】	000005108
【住所又は居所】	東京都千代田区神田駿河台四丁目 6 番地
【氏名又は名称】	株式会社日立製作所
【代理人】	
【識別番号】	100077274
【住所又は居所】	東京都新宿区西新宿1丁目23番1号 新宿千葉 ビル
【氏名又は名称】	磯村 雅俊
【復代理人】	申請人
【識別番号】	100102587
【住所又は居所】	東京都新宿区西新宿1丁目23番1号 新宿千葉 ビル
【氏名又は名称】	渡邊 昌幸

次頁無

出願人履歴情報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所